ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería Eléctrica y Computación

"Implementar un sistema de gestión de la seguridad empleando COBIT para la facultad de sistemas de la Universidad Politécnica Salesiana sede Guayaquil"

TESIS DE GRADO

Previo la obtención del Título de:

MAGISTER EN SISTEMAS DE INFORMACION GERENCIAL

Presentada por:

José Roberto Patiño Sánchez

GUAYAQUIL – ECUADOR

AÑO: 2012

AGRADECIMIENTO

A todas aquellas personas que siempre han creído en nuestra fuerza de voluntad y carácter y a las cuales esperamos nunca defraudar. Gracias por su invaluable apoyo.

DEDICATORIA

A mí querida Abuela María que me ha enseñado la tenacidad de la vida.
A mis Padres, A María N
José Patiño Sánchez

TRIBUNAL DE GRADUACIÓN

MSIG. Lenin Freire Cobos.

DIRECTOR DE TESIS

PhD. Jorge Olaya Tapia

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

(Reglamento de Graduación de la ESPOL).

José Roberto Patiño Sánchez

RESUMEN

El presente trabajo, "Implementar un sistema de gestión de la seguridad empleando COBIT para la facultad de sistemas de la Universidad Politécnica Salesiana sede Guayaquil" trata de mejorar la gestión de la seguridad de la información en dicha facultad, ajustando la misma a las condiciones locales y la necesidades de la misma optimizando los recursos que existen a través de cada capitulo se deslucirá desde la situación actual, las auditorias y los resultados:

En la primera sección se revisan los fundamentos teóricos de la gestión de seguridad de la información, así como una descripción de la estructura de la metodología COBIT utilizada para este trabajo y su comparación breve con ISO 27001 e ITIL revisando sus ventajas y desventajas.

En la segunda sección se presenta la situación actual de la universidad en lo que se refiere a la gestión y administración así como la infraestructura tecnológica. Además se realiza el análisis de riesgos de la Tecnología de la Información y se selecciona los recursos referentes a la Gestión de Seguridad de la Red Informática sobre los cuales se aplicara la auditoría, detallando el alcance de la misma, aquí también se seleccionan los procesos COBIT referentes a la Gestión de la Seguridad de la Red Informática y la descripción de las herramientas que ayudarán al desarrollo de la misma.

La tercera sección es en sí la realización de la Auditoría dividida en los cuatro grupos propuestos de procesos COBIT, y su desarrollo es basado en el documento Directrices de Auditoría COBIT a fin de determinar las fortalezas y debilidades referentes a la seguridad de la información.

La última parte da a conocer los resultados de la aplicación de la Auditoría para cada uno de los objetivos detallados de COBIT, además de un análisis del cumplimiento o no de éstos objetivos dentro de la Gestión de Seguridad de la Red Informática. Se presenta también el Informe Final de la Auditoría con los detalles más relevantes de la misma y finalmente se hace una evaluación de ciertos procesos mal gestionados detectados en el tercer capítulo.

INDICE

CAPITULO 3

CAPITULO 4

ÍNDICE DE GRÁFICOS

CAPITULO I

CAPITULO II

ÍNDICE DE CUADROS

CAPITULO II

CAPITULO III

CAPITULO IV

INTRODUCCION

Ante el esquema de globalización que las tecnologías de la información han originado principalmente por el uso masivo y universal de Internet y sus tecnologías, las entidades se ven sumergidas en ambientes agresivos donde delinquir, sabotear, robar se convierte en retos para delincuentes informáticos universales conocidos como hackers, Crackers, etc., es decir en transgresores.

La información es uno de los activos más importantes que tiene una empresa así como el recurso humano o el capital, los mismos son administrados ya sea por el área de recursos humanos, o por departamentos financieros. Pero la seguridad de información, y no hasta hace mucho, ha sido relegada de su importancia. La cual es un factor crítico para la supervivencia de las organizaciones y el cuidar de ella se vuelve más importante y necesario con el pasar del tiempo así como su gestión y continuo mejoramiento.

Últimamente, las empresas han dejado de destinar las inversiones en seguridad exclusivamente a la compra de productos (hardware y software), y comienzan a asignar parte de su presupuesto a la gestión de la seguridad de la información. El concepto de seguridad esta variando, considerando ahora la concepción de seguridad gestionada.

A medida que las tecnologías se han esparcido, la seguridad de la información está en un continuo riesgo, que obliga a la Entidad a crear medidas de emergencia y políticas decisivas para contrarrestar estos ataques y transgresiones.

Las medidas que comienzan a aplicar las empresas giran entorno al nuevo concepto de gestión de la seguridad de la información. Según la norma ISO 27002:2005 / 17799, se divide en tres vertientes: técnica, legal y organizativa, es decir, un planteamiento coherente de directrices, procedimientos y criterios que permiten a la dirección de las empresas asegurar la evolución eficiente de la seguridad de los sistemas de información, la organización afin y sus infraestructuras.

El presente proyecto de tesis muestra la realización de un proceso de Auditoria a la Gestión de Seguridad de la Red Informática mediante la

aplicación de la metodología del estándar COBIT. Tomando como base principal los aspectos señalados en su documento Directrices de Auditoría.

Este proceso se lleva a cabo con la selección de los Objetivos de Control detallados de cada uno de los Procesos COBIT que tienen relación directa con la Gestión de la Seguridad de la carrera de sistemas de la UPS sede Guayaquil, con este fin se analiza la publicación del COBIT Security Baseline para la correcta selección de dichos objetivos.

Para cada uno de estos Objetivos de Control se diseño diferentes formas de llevarlo a cabo como un programa de auditoría, una matriz de pruebas y la respectiva evaluación de éstas con las recomendaciones correspondientes. Toda esta información se presenta mediante tablas organizadas por cada dominio COBIT.

Posteriormente, se pone a consideración el análisis de resultados donde se detalla la situación actual de los procesos que cumplen con las Directrices de Auditoría COBIT, según las pruebas realizadas y sus evaluaciones.

Como resultado de lo anterior se elabora un Informe Final, donde se presenta una descripción de la situación actual de las áreas donde se encuentran las mayores debilidades en cuanto a la gestión de Seguridad de la información y se emiten recomendaciones para su atenuación o superación definitiva.

Parte adicional a este trabajo se establecerá procesos y procedimientos de seguridad que incorporan una serie de medidas sobre los activos de información de la facultad, conociendo, asumiendo y gestionando los posibles riesgos de forma documentada, estructurada, eficiente y adaptable a futuros cambios en aquellas áreas donde se identifican las principales falencias de gestión de seguridad.

Capitulo 1

1. Fundamentos Generales

1.1 Gestión de la Seguridad en redes

La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios. Tampoco deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización.[1]

Por eso es necesario la implantación de una política de seguridad en una entidad la cual requiere un estudio minucioso de todo de gestión ya sea tecnológica y/o administrativa dentro de la red; pero establecer dichas políticas conlleva al desarrollo de las organizaciones de la capacidad para afrontar ataques de cualquier tipo.

A continuación se detalla los principales aspectos a considerar en un sistema de seguridad de información, los cuales serán el fundamento del análisis de la misma:

- Gestión de riesgos

El proceso de Gestión de Riesgos es una de las piezas más importantes en un Sistema de Gestión de Información, pues conlleva a la coordinación de las actividades para dirigir y controlar una organización en torno al riesgo de seguridad de la misma.

En el proceso de Gestión de Riesgos se deberá tomar un método exhaustivo para lograr con éxito la seguridad de la información; requiriendo así la identificación de las vulnerabilidades y amenazas más comunes a las cuales la empresa u organización está sujeta, a la cuantificación del daño potencial que podría existir frente a dichas amenazas y el desarrollo de pasos y procedimientos de mitigación para lograr un nivel de riesgo tolerable.

- La gestión de Seguridad

Se refiere a la habilidad para supervisar y controlar la disponibilidad de facilidades de confiabilidad, y a reportar amenazas y rupturas en la misma.

Pero también involucra a la seguridad de la gestión, que requiere de la habilidad para autentificar usuarios y aplicaciones de gestión, para así garantizar la confidencialidad e integridad e integridad la información.

- Políticas de Seguridad

Se entiende como un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información, puede cubrir cualquier cosa desde buenas prácticas para la seguridad de un solo ordenador, reglas de una empresa o edificio. Contiene la definición de la seguridad de la información bajo el punto de vista de cierta entidad[1].

Debe ser enriquecida y compatibilizada con otras políticas dependientes de ésta, objetivos de seguridad, procedimientos. Debe estar fácilmente accesible de forma que los empleados estén al tanto de su existencia y entiendan su contenido. Puede ser también un documento único o inserto en un manual de seguridad. Se debe designar un propietario que será el responsable de su mantenimiento y su actualización a cualquier cambio que se requiera, usualmente involucrado con la alta dirección.

[1] Tomado del Wikipedia, enciclopedia libre

Para que una política de seguridad se considere efectiva deberá tener en cuenta seis elementos claves para garantizar la información del sistema:

- Disponibilidad

Es el acceso a la información y sus activos asociados por parte de los usuarios autorizados cuando lo requieran.

- No Repudio

Consiste en evitar que el emisor o el receptor nieguen la transmisión de un mensaje. Así, cuando se envía un mensaje, el receptor puede comprobar que, efectivamente, el supuesto emisor envió el mensaje. De forma similar, cuando se recibe un mensaje, el emisor puede verificar que, de hecho, el supuesto receptor recibió el mensaje.

- Confidencialidad

Acceso a la información por parte únicamente de quienes están autorizados [2].

- Autenticidad

Corresponde al hecho que el o los sistemas han de ser capaces de verificar la identidad de sus usuarios, y los usuarios la del sistema.

La autenticación concierne al aseguramiento de que una comunicación es autentica. En el caso de un mensaje sencillo, como una alarma o una advertencia, la función del servicio de autenticación es asegurar al receptor que el mensaje es del emisor original. En el caso de una interacción que puede ser un inicio de conexión, el servicio asegura que las dos entidades

son autenticas, es decir, que cada una es la entidad que dice ser.

- Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

- Control de Acceso

En el contexto de la seguridad de red, el control de acceso es la habilidad para limitar y controlar el acceso al sistema host y aplicaciones vía enlaces de comunicación. Para lograr este control cada entidad tratando de tener acceso debe primero ser identificada, o legitimada, tal que los derechos de acceso pueden ser ajustados al individuo.

El proceso de Gestión de Riesgos es una de las piezas más importantes en un Sistema de Gestión de Información, pues conlleva a la coordinación de las actividades para dirigir y controlar una organización en torno al riesgo de seguridad de la misma[1].

En el proceso de Gestión de Riesgos se deberá tomar un método exhaustivo para lograr con éxito la seguridad de la información; requiriendo así la identificación de las vulnerabilidades y amenazas más comunes a las cuales la empresa u organización está sujeta, a la cuantificación del daño potencial que podría existir frente a dichas amenazas y el desarrollo de pasos y procedimientos de mitigación para lograr un nivel de riesgo tolerable.

➢ Análisis de Riesgos

El análisis de riesgos trata sobre como minimizar los efectos de un problema de seguridad; para esto se debe tener identificado claramente que es lo que se quiere proteger, contra que, y como se lo va a resguardar.

Se conocen dos alternativas, una cuantitativa y otra cualitativa.

El análisis mas aceptado es el cualitativo, últimamente muy difundido por las llamadas "consultoras de seguridad", que se especializan en seguridad lógica, ips, tests de infiltración y similares. Este método toma en consideración realizar estimaciones de perdidas potenciales, para lo cual relacionan cuatro puntos importantes:

- Las amenazas
- Las vulnerabilidades
- El impacto asociado a una amenaza
- Los controles o salvaguardas.

Se puede obtener un indicador cualitativo del nivel de riesgo asociado a un activo determinado dentro de la organización, visto como la probabilidad de que una amenaza se materialice sobre un activo y produzca un determinado impacto.

➢ Identificación de Recursos

Donde se identifican todos los recursos cuya integridad pueda ser amenazada de la siguiente o de cualquier forma:

- Hardware
- Software
- Información
- Personas
- Accesorios

- Identificación de Amenazas y Vulnerabilidades

Luego de la identificación de recursos a proteger se deben reconocer las vulnerabilidades y amenazas a que están expuestos. Una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y una amenaza es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad; entre ambas existe una estrecha relación: sin vulnerabilidades no hay amenazas, y sin amenazas no hay vulnerabilidades.

Las amenazas se catalogan en diferentes grupos y no solo centrarse en ataques externos sino también internos y accidentales según su impacto sobre los sistemas informáticos y la forma como se producen:

- Desastres del entorno

Se refieren a problemas relacionados con la ubicación del entorno de trabajo informático o de la propia organización, así como con las personas que de una u otra forma están relacionadas con el mismo. Se toman en cuenta desastres naturales (terremotos, inundaciones, etc.), desastres producidos por elementos cercanos, como los cortes de fluido eléctricos, y peligros relacionados con operadores, programadores o usuarios del sistema.

- Amenazas en el sistema

Se refieren a todas las vulnerabilidades de los equipos y su software que pueden acarrear amenazas a la seguridad, como fallos en el sistema operativo, medidas de protección que este ofrece, fallos en los programas, copias de seguridad, etc.

- Amenazas en la red

Se debe tener en cuentas los aspectos relativos al cifrado de los datos que son sujetos de transmisión, protección de una red local

de Internet, sistemas de legitimación de usuarios remotos que accedan a ciertos recursos de la red interna.

- Medidas de Protección

En primer lugar se debe cuantificar los daños que cada posible vulnerabilidad puede causar teniendo en cuenta las posibilidades de que una amenaza se pueda convertir en realidad. Este cálculo puede partir de hechos sucedidos con anterioridad en la organización.

La categorización de riesgos es fundamental para analizar medidas de protección que suelen realizarse en base al nivel de importancia del daño causado y a la probabilidad aproximada de que ese daño se convierta en realidad; se trata principalmente de no gastar mas dinero en una implementación para proteger un recurso de lo que vale o de lo que costaría recuperarse de un daño o de su perdida total. Evidentemente, los recursos que presenten un riesgo evaluado mayor serán los que más medidas de protección deben poseer, ya que aquello significa que es probable que sean atacados, y que además el ataque puede causar perdidas importantes.

Como un riesgo es imposible de eliminarlo completamente se lo puede minimizar, por lo que se debe planificar no solo la prevención de que una amenaza se realice (medidas proactivas), sino también el procedimiento para recuperarse del ataque si este se produce (medidas reactivas) [3].

- Estrategias de respuesta

Existen dos estrategias de respuesta ante un incidente de seguridad:

  - Proteger y proceder.

    Se aplica cuando la organización es muy vulnerable o el nivel de los atacantes es elevado; la filosofía es proteger de manera inmediata la red y los sistemas y restaurar su estado normal, de forma que los usuarios puedan seguir trabajando normalmente. Será necesario interferir de forma activa las acciones del intruso

para evitar más accesos, y analizar el daño causado. La principal desventaja de esta estrategia es que el atacante se da cuenta rápidamente de que ha sido descubierto, y puede emprender acciones para no ser identificado, lo que incluso conduce al borrado de logs o de sistemas de ficheros completos; incluso puede cambiar su estrategia de ataque a un nuevo método, y seguir comprometiendo al sistema. Sin embargo, esta estrategia también presenta una parte positiva: el bajo nivel de conocimientos de los atacantes en sistemas habituales hace que en muchas ocasiones se limiten a abandonar su ataque[2].

- Perseguir y procesar

Adopta la filosofía de permitir al atacante proseguir sus actividades, pero de forma controlada y observada por los administradores, de la forma mas discreta posible. Con esto, se intentan guardar pruebas para ser utilizadas en la segunda parte de la estrategia, la de acusación y procesamiento del atacante (ya sea ante la justica o ante los responsables de la organización, si se trata de usuarios internos). Se corre el peligro de que el intruso descubra su monitorización y destruya complemente el sistema, así como que los resultados no se tengan en cuenta ante un tribunal debido a estrategias legales; la parte positiva de esta estrategia es, aparte de la recolección de pruebas, que permite a los responsables conocer las actividades del atacante, que vulnerabilidades de la organización ha aprovechado para atacarla, como se comporta una vez dentro, etc. De esta forma se aprovecha el ataque para reforzar los puntos débiles de los sistemas. [4]

1.2 El estándar COBIT como metodología

Antes de empezar a analizar al COBIT como metodología se debe conocer los demás estándares del mercado como el ITIL e ISO/IEC

[2] http://spi1.nisu.org/recop/al01/javier/part4.html

27002 para luego profundizar más en el estándar escogido para esta tesis.

ITIL

Hoy, las organizaciones dependen de las TI para satisfacer sus objetivos corporativos y sus necesidades de negocios, entregando valor a sus clientes. Para que esto ocurra de una forma gestionada, responsable y repetible, la empresa debe asegurar que los servicios recibidos de alta calidad de TI deben:

- Satisfacer las necesidades de la empresa y los requisitos de los usuarios.
- Cumplir con la legislación.
- Asignarse y entregarse de forma eficaz y eficiente.
- Revisarse y mejorarse de forma continua.

La gestión de servicios de TI se refiere a la planificación, aprovisionamiento, diseño, implementación, operación, apoyo y mejora de los servicios de TI que sean apropiados a las necesidades del negocio. ITIL proporciona un marco de trabajo de mejores prácticas integral, consistente y coherente para la gestión de servicios de TI y los procesos relacionados, la promoción de un enfoque de alta calidad para el logro de la eficacia y eficiencia del negocio en la gestión de servicios de TI.

ITIL intenta respaldar mas no fijar los procesos de negocio de una organización. En este contexto, la OGC no aprueba el término "Cumplimiento con ITIL". El papel del marco de trabajo de ITIL es describir los enfoques, las funciones, los roles y procesos en los que las organizaciones pueden basar sus propias prácticas. El rol de ITIL es brindar orientación en el nivel organizacional más bajo que pueda aplicarse.
Debajo de ese nivel, para implementar ITIL en una organización se requieren los conocimientos específicos de sus procesos de negocio para ajustar ITIL a fin de lograr una eficacia óptima.

Es útil pensar en la estructura de gestión de servicios como una pirámide con el estándar internacional ISO/IEC 20000:2005 en la cima (**Figura 1**). Se trata de una especificación formal y las organizaciones pueden obtener la acreditación para demostrar el

cumplimiento con la norma. Por debajo de la cima está la capa de mejores prácticas de ITIL, que ayuda a asegurar y demostrar que las disposiciones de la norma se están cumpliendo. De manera similar, los procesos de ITIL pueden ser utilizados para lograr y demostrar el cumplimiento con los objetivos de control COBIT (la función de los apéndices del presente documento es mostrar la relación entre las dos estructuras). Así que si ITIL es la capa intermedia, la adaptación de ITIL para satisfacer las necesidades de una organización en particular es el nivel más bajo, la base más amplia de la implementación de ITIL[3].

GRAFICO 1.1

RELACION DE ITIL/ISO CON LOS REQUERIMIENTOS DEL NEGOCIO

[3] http://www.iso.org

GRAFICO 1.2

TOPICOS PRINCIPALES ITIL

Figura 3 — Topicos principales ITIL				
Estrategia de Servicio (SS)	**Diseño del Servicio (SD)**	**Transición del Servicio (ST)**	**Operación del Servicio (SO)**	**Mejora Continua del Servicio (CSI)**
• Gestión del servicio • Ciclo de vida del servicio • Activos del servicio y creación de valor • Tipos y estructuras de proveedores de servicios • Estrategia, mercados y oferta • Gestión financiera • Gestión del portafolio de servicios • Gestión de la demanda • Diseño organizacional, cultura y desarrollo • Estrategia de aprovisionamiento • Automatización e interfaces de servicios • Herramienta para estrategias • Desafíos y riesgos	• Diseño balanceado • Requisitos, indicadores, actividades y limitantes • Arquitectura orientada al servicio • Gestión de servicios de negocio • Modelos de diseño de servicios • Gestión del catálogo de servicios • Gestión de niveles de servicios • Capacidad y disponibilidad • Continuidad de servicios de TI • Seguridad de la información • Gestión de proveedores • Gestión de datos y de la información • Gestión de aplicaciones • Roles y herramientas • Análisis de impacto en el negocio • Desafíos y riesgos • Paquete de diseño de servicios • Criterios de aceptación de servicios • Documentación • Aspectos ambientales • Marco de trabajo de maduración de procesos	• Objetivos, principios, políticas, contexto, roles y modelos • Planificación y soporte • Gestión del cambio • Activos del servicio y gestión de la configuración • Liberación y distribución • Validación y prueba del servicio • Evaluación • Gestión del conocimiento • Gestionando las comunicaciones y el compromiso • Gestión de partes interesadas • Sistema de gestión de configuraciones • Introducción por etapas • Desafíos y riesgos • Tipos de activos	• Equilibrio en la operación del servicio • Salud operacional • Comunicación • Documentación • Eventos, incidentes y problemas • Atención de requerimientos • Gestión de accesos • Monitoreo y control • Gestión de la infraestructura y el servicio • Gestión de instalaciones y del Data Center • Seguridad física y de la información • Mesa de servicios • Gestión técnica de operaciones de TI y de aplicaciones • Roles, responsabilidades y estructuras organizacionales • Soporte tecnológico a la operación del servicio • Gestionando los cambios, proyectos y riesgos • Desafíos • Guía complementaria	• Objetivos, métodos y técnicas • Cambio organizacional • Propiedad • Drivers • Gestión de niveles de servicios • Medición del servicio • Gestión del conocimiento • Benchmarking • Modelos, estándares y calidad • Proceso de mejoramiento de los siete pasos CSI • Retorno sobre la inversión (ROI) y aspectos de negocio • Roles • Matriz RACI • Herramientas de soporte • Implementación • Gobierno • Comunicaciones • Desafíos y riesgos • Innovación, corrección y mejoramiento • Apoyo de las mejores prácticas a la mejora continua del servicio (CSI)

También hay un volumen introductorio6 que describe la justificación del modelo de ciclo de vida y abarca los principios fundamentales en cada etapa del ciclo de vida. Existen otras publicaciones de apoyo y otros títulos en preparación. El editor oficial de OGC es The Stationery Office (TSO), que publica ITIL en libros, libros electrónicos y archivos PDF, o mediante suscripción en línea. TSO también maneja una biblioteca de publicaciones de apoyo y complementarios y un sitio web de las mejores prácticas para ITIL y otros productos de mejores prácticas de OGC[4].

El esquema de calificación de ITIL ofrece la certificación de las personas, que van desde una apreciación a nivel de fundamentos de

[4] http://www.bestmanagementpractice.com

los términos y conceptos de ITIL hasta un título profesional avanzado. El acreditador oficial de OGC es APM Group, que licencia a una serie de institutos para ofrecer exámenes, gestionar y acreditar a las organizaciones de formación.[5]

Desde 1991, ITIL ha sido patrocinado y apoyado por itSMF, un proveedor y grupo de usuarios que ahora tiene capítulos en más de 40 países de todo el mundo. Es una organización sin fines de lucro y un actor importante en el desarrollo continuo y promoción de las mejores prácticas en la gestión, estándares y calificaciones de servicios TI. El itSMF provee una red accesible de expertos de la industria, fuentes de información y eventos para ayudar a los países miembros a abordar los problemas de gestión de servicios de TI y lograr la entrega de servicios consistentes, de alta calidad, internos y externos, a través de la adopción de mejores prácticas. A nivel mundial, el itSMF ahora cuenta con más de 6.000 empresas asociadas, públicas y privadas, que incluyen más de 70.000 personas[4].

ISO/IEC 27002

El estándar internacional fue publicado por la ISO (*www.iso.org/ISO/home.htm*) y la IEC, que establecieron el comité técnico mixto ISO/IEC JTC 1. La fuente histórica para el estándar fue BS 7799-1, cuyas partes esenciales fueron tomadas en el desarrollo de la norma ISO/IEC 17799:2005 Tecnología de la Información – Código de Prácticas para la Gestión de Seguridad de la Información. Fue desarrollado y publicado por la British Standards Institution (BSI), denominado como BS 7799-1:1999. El estándar original inglés se publicó en dos partes:

- BS 7799 Parte 1: Tecnologías de la Información – Código de Prácticas para la Gestión de Seguridad de la Información.
- BS 7799 Parte 2: Sistemas de Gestión de Seguridad de la Información – Especificaciones con guías para su uso.

La norma publicó su primera edición en el año 2000 y actualizada en junio de 2005. Se puede clasificar como las mejores prácticas actuales en materia de sistemas de gestión de seguridad de la información. La BS 7799 original fue revisada y reeditada en septiembre de 2002. A menudo se utiliza ISO/IEC 27002 como un

[4] http://www.itsmfi.org

término genérico para describir lo que actualmente son dos documentos diferentes:

- ISO/IEC 17799 (ahora renombrada como ISO 27002, un conjunto de controles de seguridad (un código de práctica).
- ISO/IEC 27001 (anteriormente, BS7799-2) – Una especificación estándar para un sistema de gestión de seguridad de información (SGSI).

El objetivo del estándar ISO/IEC 27002:2005 es brindar información a los responsables de la implementación de seguridad de la información de una organización. Puede ser visto como una buena práctica para desarrollar y mantener normas de seguridad y prácticas de gestión en una organización para mejorar la fiabilidad en la seguridad de la información en las relaciones interorganizacionales. En él se definen las estrategias de 133 controles de seguridad organizados bajo 11 dominios. La norma subraya la importancia de la gestión del riesgo y deja claro que no es necesario aplicar cada parte, sino sólo aquellas que sean relevantes.

Los principios rectores en la norma ISO/IEC 27002:2005 son los puntos de partida para la implementación de seguridad de la información. Se basan en cualquiera de los requisitos legales o en las mejores prácticas generalmente aceptadas.

Las mediciones basadas en los requisitos legales son:

- La protección y la no divulgación de datos personales.
- Protección de la información interna.
- Protección de los derechos de propiedad intelectual.

Las mejores prácticas mencionadas en la norma incluyen:

- La política de seguridad de la información.
- Asignación de la responsabilidad de seguridad de la información.
- Escalamiento de problemas.
- Gestión de la continuidad del negocio.

Cuando se implementa un sistema de gestión de seguridad de la información, se deben considerar varios factores críticos de éxito:

- La política de seguridad, sus objetivos y actividades deberían reflejar los objetivos de negocio.

- La implementación debería considerar los aspectos culturales de la organización.
- Se requiere un abierto apoyo y el compromiso de la alta dirección.
- Se requiere un conocimiento exhaustivo de los requisitos de seguridad, evaluación del riesgo y gestión del riesgo.
- El marketing efectivo de la seguridad debe dirigirse a todo el personal, incluidos los miembros de la dirección.
- La política de seguridad y las medidas de seguridad deben ser comunicadas a terceros contratados.
- Los usuarios deben ser capacitados en forma adecuada.
- Se debería disponer de un sistema integral y balanceado para la medición del desempeño, que apoye la mejora continua de suministro de información.[6]

Después de presentar información introductoria (ámbito de aplicación, términos y definiciones), se debe presentar un marco de trabajo para el desarrollo de un Sistema de Gestión de Seguridad de Información específico para la empresa, que debería consistir de al menos los siguientes componentes:

- La política de seguridad.
- Organización para la seguridad.
- Clasificación de activos y su control.
- Seguridad del personal.
- Seguridad física y ambiental.
- Comunicaciones y gestión de operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Gestión de la continuidad del negocio.
- Cumplimiento.

COBIT

COBIT es un marco de referencia globalmente aceptado para el gobierno de TI basado en estándares de la industria y las mejores prácticas. Una vez implementado, los ejecutivos pueden asegurarse de que se ajusta de manera eficaz con los objetivos del negocio y dirigir mejor el uso de TI para obtener ventajas comerciales. COBIT brinda un lenguaje común a los ejecutivos de negocios para

comunicar las metas, objetivos y resultados a los profesionales de auditoría, informática y otras disciplinas.

COBIT brinda las mejores prácticas y herramientas para el monitoreo y la gestión de las actividades de TI.

El uso de las TI es una inversión importante que debe ser gestionado. COBIT ayuda a los ejecutivos a comprender y gestionar las inversiones de TI durante su ciclo de vida y proporciona un método para evaluar si los servicios de TI y las nuevas iniciativas satisfacen los requisitos empresariales y sea probable que entreguen los beneficios esperados.

Debido a que COBIT es un conjunto de herramientas y técnicas probadas y aceptadas internacionalmente, su implementación es una señal de buena gestión en una organización. Ayuda a los profesionales de TI y a usuarios de empresas a demostrar su competencia profesional a la alta dirección. Como ocurre con muchos procesos de negocio genéricos, existen estándares y mejores prácticas de la industria de TI que las empresas deberían seguir cuando utilizan las TI. COBIT se nutre de estas normas y proporciona un marco para implementarlas y gestionarlas.

Una vez que se identifican e implementan los principios clave de COBIT para una empresa, los ejecutivos ganan confianza en que la utilización de las TI puede ser gestionada de forma eficaz.

Las versiones 4.x de COBIT, incluyen lo siguiente:

- Marco de trabajo: Explica cómo es que COBIT organiza la gestión del gobierno de TI, los objetivos de control y las mejores prácticas de los procesos y dominios de TI, y los relaciona con las necesidades del negocio. El marco contiene un conjunto de 34 objetivos de control de alto nivel, uno para cada proceso de TI, agrupados en cuatro dominios: Planificar y Organizar, Adquirir e Implementar, Entregar y dar soporte, Monitorear y Evaluar.
- Las descripciones del proceso incluyen cada uno de 34 procesos de IT, cubriendo las áreas de responsabilidad de la empresa y de TI desde el principio hasta el final.
- Los objetivos de control proveen los objetivos de gestión de las mejores prácticas genéricas para los procesos de TI.
- Las directrices de gestión ofrecen herramientas para ayudar a asignar responsabilidades y medir el desempeño.[10]

- El modelo de madurez proporciona perfiles de los procesos de TI que describen los posibles estados actuales y futuros.
- Las publicaciones adicionales de soporte están disponibles para ayudar en la orientación en la puesta en práctica, lograr el aseguramiento y lidiar con aspectos específicos tales como la seguridad. Val IT5 ha sido desarrollado para concentrarse específicamente en la entrega de valor del gobierno de TI[6].

➢ Historia del COBIT

ISACF (Information System Audit and Control Fundation), es una comunidad de profesionales, fundada en 1976 que tiene como propósito realizar trabajos de investigación con el fin de incrementar el conocimiento y valor sobre el control, Aseguramiento y Gobierno de la Tecnología de Información. En 1998, se instaura el instituto de Gobierno de la tecnología de Información (IT Governance Institute), destinado a enriquecer el entendimiento y promover la adopción de los principios del Gobierno de TI.

Para 1996, ISACF emite una publicación sobre Objetivos de Control para la información y tecnologías relacionadas. Una segunda edición revisada y que agrega un Conjunto de Herramientas de Implementación fue liberada en 1998.

COBIT (Control Objetives Information Tecnologies – Objetivo de Control para Tecnología de Información), constituye la tercera edición de los Objetivos de Control cuyo editor principal fue el instituto de Gobierno de TI, creado así una herramienta de Gobierno de Tecnología de la Información, que vincula la tecnología informática y practicas de control, además consolida estándares de fuentes globales confiables en un recurso esencial para la administración (gerencia), los usuarios (profesionales de control) y los auditores.

➢ Misión

El organismo de Control y Auditoria, ISACA (Information Systems Audit And Control Association) y el comité Directivo de COBIT han definido la misión del estándar así:

[6] http://www.isaca.org

"Investigar, desarrollar, publicar y promover un conjunto de objetivos de control en tecnología de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso cotidiano de gerentes de empresas y auditores." [7]

- **Alcance**

Orientado al negocio (Gerencia).

Alineado con estándares y regulaciones de hecho y de derecho.

Basado en normas revisadas crítica y analíticamente para ser aceptadas en las tareas y actividades de TI.

Alineado con estándares de control y auditoria (COSO, IFAC, IIA, ISACA, AICPA).

Aplicable a las funciones de Servicios de Sistemas de Información de toda la empresa.

- **Objetivos**

- Proporcionar a la Gerencia de normas basadas en buenas prácticas para el control de la información y la Tecnología de la Información, lo que incluye a la seguridad informática. COBIT es la herramienta de Gobierno de TI que ayude al entendimiento y a la administración de los riesgos así como de los beneficios asociados con la información y sus tecnologías relacionadas.
- Dar a los usuarios una base confiable para administrar los recursos de TI.
- Proveer a los auditores de buenos criterios para las tareas de evaluación, control y auditoria.
- Suministrar a la gerencia, responsables de procesos de negocio y auditores, el respaldo suficiente para mejorar la administración de la IT: COBIT esta diseñado para ser utilizado por los propietarios de los procesos de negocio como una guía clara y entendible para que estos tengan total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio.

➢ Audiencia

Particularmente, se reconoce que COBIT puede ser útil para diferentes miembros o entes dentro de una organización, así:

La Gerencia: en lo referente a la toma de decisiones de inversión en TI y control, para analizar el costo-beneficio del control en un ambiente de riesgos impredecibles.

Los usuarios Finales: para contar con una garantía sobre la seguridad, calidad y el control de los productos de TI internos y adquiridos.

Los Auditores: para apoyar sus opiniones sobre los controles de los proyectos de TI, su injerencia en la empresa y determinar el nivel de control requerido.

➢ Estructura del estándar COBIT

El estándar consta principalmente de 4 libros que sirven como guía para alcanzar los objetivos planteados por la Administración, Usuarios y Auditores, además de un conjunto de Herramientas y Guías para ejecutar la implementación y soportar la administración.

- Resumen Ejecutivo
- Marco de Referencia
- Objetivos de Control
- Guías de Auditoría
- Herramientas de Implementación
- Guías de Administración

➢ Resumen Ejecutivo

Provee a la Administración del conocimiento de los principios y conceptos esenciales de COBIT. Ya que de ello depende el optimizar el empleo de los recursos disponibles (personal, instalaciones, sistemas de aplicaciones y datos) para cumplir con esta responsabilidad y alcanzar sus objetivos. La administración debe

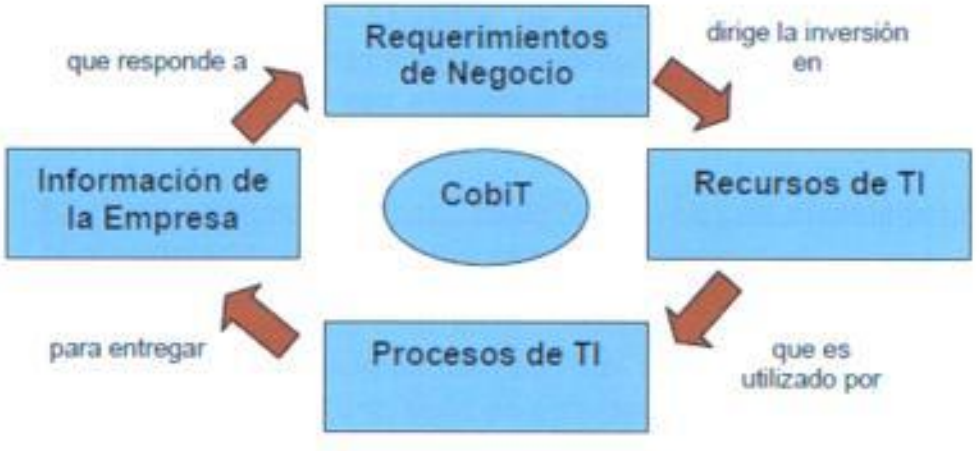
comprender el estado de sus propios sistemas de TI y decidir el nivel de seguridad y control que deben proveer estos sistemas.

- **Marco de Referencia**

El Marco referencial COBIT se fundamenta en que el enfoque de control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio. La información es el resultado de la aplicación combinada de negocio. La información es el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información, que deben ser administrados por procesos de TI. Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como Requerimientos de Negocio para la información.

GRAFICO 1.3

RELACION DE LOS PROCESOS Y RECURSOS DE TI CON LOS REQUERIMIENTOS DEL NEGOCIO



COBIT ha definido los siguientes requerimientos del Negocio:

- REQUERIMIENTOS DE CALIDAD: Calidad, Costo, Entrega de Servicio.
- REQUERIMIENTOS FIDUCIARIOS: Efectividad y Eficiencia de Operaciones, Confiabilidad de la Información, Cumplimiento de las leyes y regulaciones.
- REQUERIMIENTOS DE SEGURIDAD: Confidencialidad, Integridad y Disponibilidad.

La Calidad ha sido considerada principalmente por su aspecto negativo (no fallas, confiabilidad, etc), lo que implica criterios de integridad. Está dirigida al manejo apropiado de los riesgos contra las oportunidades. El aspecto de calidad está cubierto por los criterios de efectividad. Se considera que el aspecto de disponibilidad correspondiente a los requerimientos de seguridad y también en alguna medida, con la efectividad y la eficiencia.

Para los Requerimientos Fiduciarios, se utilizaron definiciones de COSO (Committe of Sponsoring Organisations of the Treadway Commission Internal Control-Integrates Framework) para la efectividad y eficiencia de operaciones, confiabilidad de información y cumplimiento con leyes y regulaciones.

Con respecto a los aspectos de seguridad, COBIT identificó la confidencialidad, integridad y disponibilidad como los elementos clave, que son los tres elementos utilizados a nivel mundial para describir los requerimientos de seguridad.

El marco referencial se clasifica en tres niveles de actividades de TI al considerar la administración de sus recursos.

En la base se encuentran las actividades y las tareas necesarias para obtener un resultado medible. Los procesos se definen en un nivel superior como una serie de actividades o tareas conjuntas con cortes de control. En el nivel más alto, los procesos son agrupados en dominios. Su agrupamiento corresponde a la responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo aplicable a los procesos de TI.

Grafico 1.4

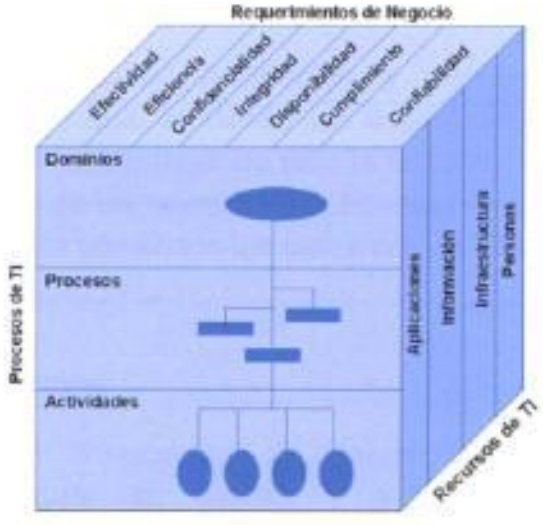
NIVELES DEL MARCO REFERENCIAL

Fuente: Marco referencial del COBIT 4.1

Básicamente, el Marco Referencial puede ser enfocado desde tres puntos clave: Los criterios de Información, Los Recursos de TI, y los Procesos de TU. Lo cual, se puede distinguir en el Cubo COBIT que se muestra a continuación.[9]

Grafico 1.5

CUBO COBIT DE PUNTOS ESTRATÉGICOS



Fuente: Marco Referencial COBIT 4.1

Con lo anterior, se puede conocer en detalle los 34 Objetivos de Control de alto nivel, definidos para cada uno de los Procesos de Ti, agrupados en cuatro dominios: Planificación y Organización, Adquisición e Implementación, Entrega de Servicios y, Soporte y Monitoreo.

Las definiciones para los Dominios identificados son:

- Planeación y Organización

Se refiere a las estrategias y tácticas; a la manera como la Tecnología de Información apoya al logro de los objetivos de la empresa. Se añade también la necesidad de que la visión estratégica debe ser planeada, comunicada, y administrada desde diferentes puntos de vista.

- Adquisición e Implementación

Para poner en ejecución la estrategia de TI, es necesario identificar las soluciones de TI, sean estás desarrolladas o adquiridas, además deben ser implementadas e integradas dentro del proceso del negocio. Este dominio abarca también los cambios a sistemas existentes para asegurar la continuidad de su ciclo de vida.

- Entrega y Soporte

Corresponde a la distribución y entrega de los servicios requeridos lo que va desde las actividades cotidianas hasta el entrenamiento, sin dejar de lado la seguridad de los sistemas y la continuidad de las operaciones. Este dominio abarca los procesos a los que son sometidos los datos por los sistemas de aplicación.

- Monitoreo

Se refiere a la necesidad de evaluar los procesos regularmente para asegurar su calidad y suficiencia referencia a los requerimientos de control. Toma también en cuenta la necesidad

de crear procesos de control independientes, generalmente estos son llevados a cabo por auditorías internas y externas.

- Objetivos de Control

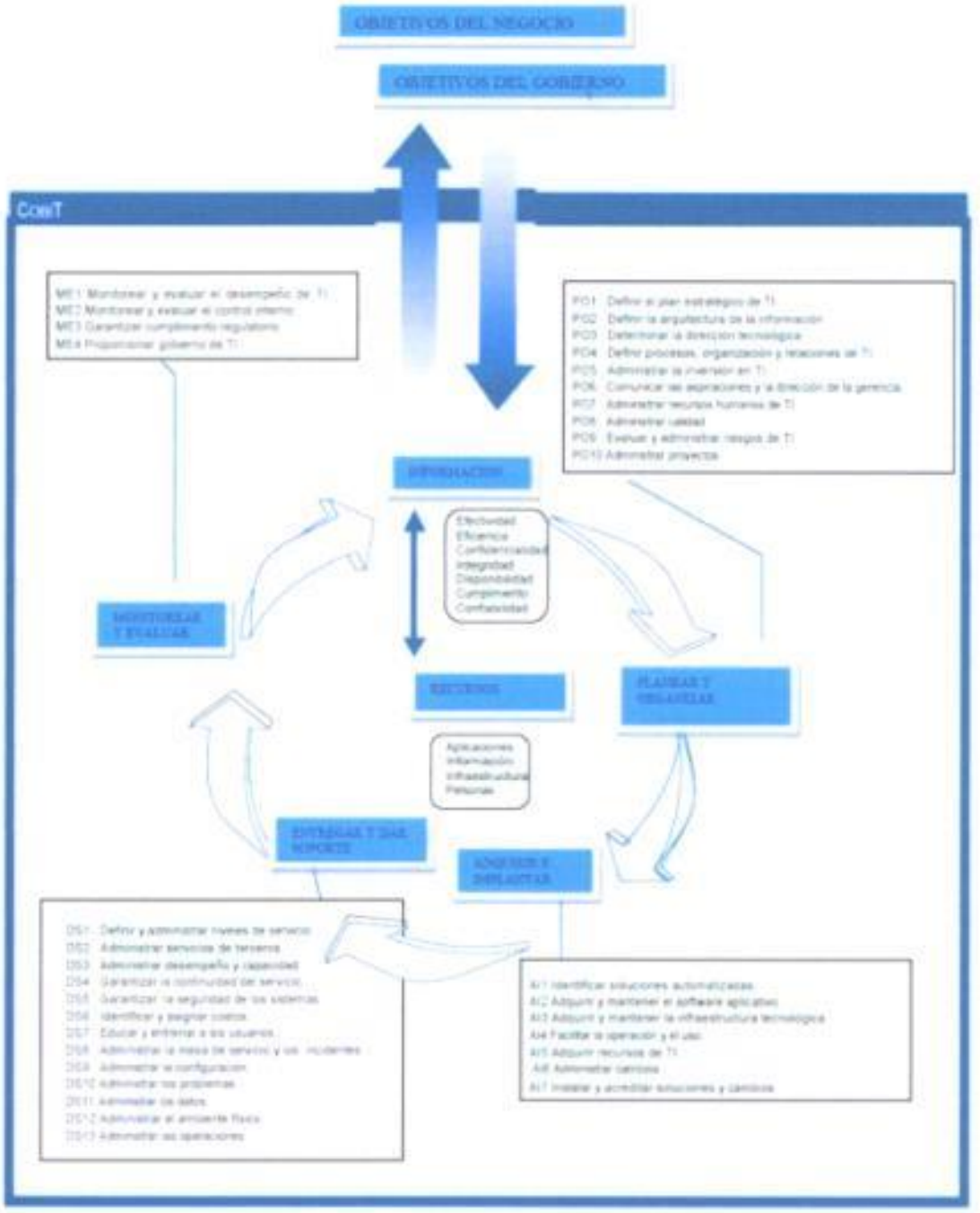
Objetivos de Control son la base del conjunto de conocimientos requerido para soportar la auditoría y control de los sistemas de información.

Los Objetivos de Control de TI han sido organizados por proceso/actividad y también se han proporcionado dos ayudas de navegación para facilitar la entrada a partir de cualquier punto de vista estratégico y para facilitar enfoques combinados o globales, tales como instalación/implementación de un proceso responsables gerenciales globales para un proceso y utilización de recursos de TI por un proceso. [8]

Los Objetivos de Control se enfocan sobre Objetivos de control detallados y específicos asociados a cada proceso de TI. Por cada uno de los 34 procesos de TI del marco referencial, hay desde tres hasta 30 objetivos de control detallados, para un total de 318.

Grafico 1.6

PROCESOS DE IT DE COBIT DEFINIDOS DENTRO DE LOS CUATRO DOMINIOS



➢ Guías o Directrices de Auditoría

Las Directrices de Auditoría proporcionan guías para preparar planes de auditoría que se integran al Marco referencial de COBIT y a los Objetivos de Control detallados. Deben ser usado conjuntamente con estos dos últimos, y a partir de ahí pueden desarrollarse programas específicos de auditoría.

Sin embargo, las Directrices no son exhaustivas ni definitivas. No pueden incluir todo ni ser aplicables a todo, así que deberán ajustarse a condiciones específicas. [12]

La preparación de estos programas esta basada en:

- Adquirir conocimiento a través de entrevistas.
- Considerar y evaluar la conveniencia de los controles establecidos.
- Valorar la suficiencia de los procesos.
- Justificar el riesgo de que los objetivos de control no se alcancen.

Las Guías de Auditoría también para cada uno de los 34 objetivos de control, que permitirán la revisión de los procesos de TI contra los 318 objetivos de control detallados y que aseguran a la Gerencia el cumplimiento o mejoramiento de los mismos.

➢ Herramientas de Implementación

El conjunto de Herramientas de Implementación presentan una documentación sobre la evaluación de la exitosa aplicación de COBIT en ambientes de trabajo de diferentes empresas para que las utilicen los demás. [11]

El conjunto de Herramientas de Implementación contiene:

- Resumen Ejecutivo
- Guía para la Implementación, incluyendo una muestra de memorándums y presentaciones.
- Diagnósticos de Sensibilización de la Administración y Diagnósticos de Control de TI
- Casos de Estudio describiendo la implementación del COBIT

- Las Preguntas más comunes y las Respuestas
- Presentaciones de Power Point implementar/vender el COBIT

➢ Guías o Directrices Gerenciales o de Administración

Estas directrices han sido desarrolladas recientemente y su objetivo es ayudar a la Gerencia a cumplir con las necesidades y requerimientos del Gobierno de TI de una manera más efectiva.

Estas directrices son:

Factores Críticos de Éxito.- donde se definen las directrices más importantes que deben ser tomadas en cuenta por la Administración para tener el control sobre los procesos de TI.

Modelo de Madurez.- para controlar los procesos de TI, y así la Administración pueda ubicar a su empresa en el entrono actual, con referencia a su competencia, en la industria, y con los estándares internacionales.

Indicadores Clave por Objetivo.- donde se definen los mecanismos de valoración, que indicarán a la Gerencia si un proceso de TI ha satisfecho los requerimientos del negocio.

Indicadores Claves de Desempeño.- son los indicadores principales que definen el valor para conocer que tan bien se está ejecutando un proceso de TI frente al objetivo que se busca.

Las Directrices Gerenciales son consistentes con y se basan en el Marco Referencial de COBIT, los Objetivos de Control y las Directrices de Auditoría de COBIT existentes.

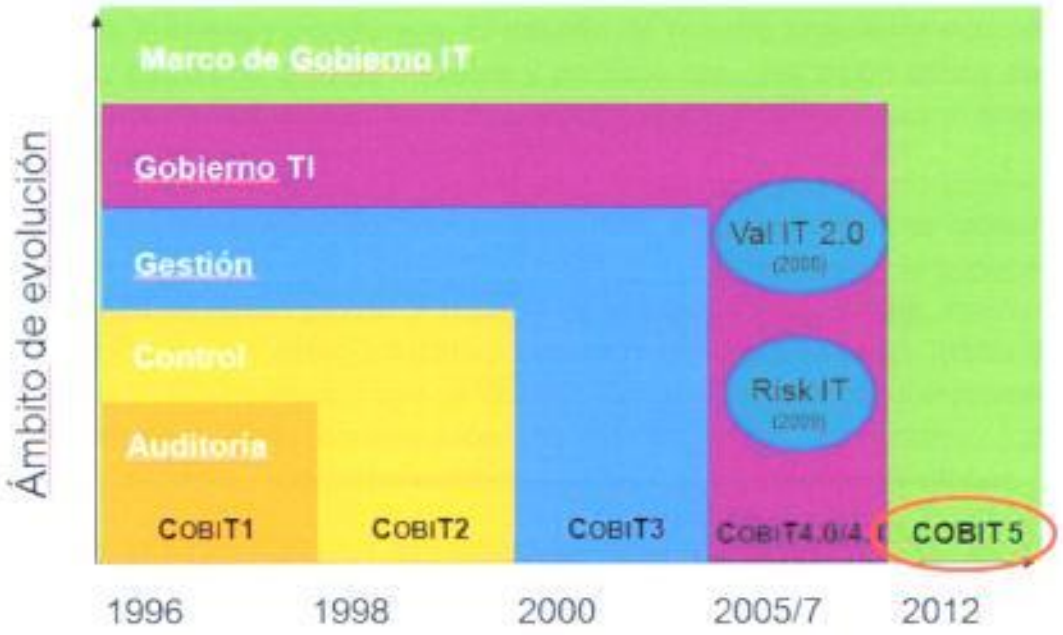
➢ Comparación Cobit 4.1 vs 5.0

ISACA liberó la documentación final, así que parece conveniente revisar las novedades que incluye esta esperada actualización la nueva versión tiene un carácter clarificador, integrando COBIT 4, Val IT y RISK IT en su modelo de referencia de procesos. Asimismo,

COBIT 5 ha sido adaptado para alinearse con la norma ISO/IEC 38500 de Gobierno TI y con el marco GEIT del ITGI (IT Governance Institute). El nuevo modelo se basa en los siguientes elementos: 5 Principios Satisfacer las necesidades de los Stakeholders (Interesados) Crear valor manteniendo el equilibrio entre realización de beneficios y la optimización del uso de recursos y gestión del riesgo. Cubrir la organización de principio a fin. Integrando el Gobierno corporativo con el Gobierno de las TI. Orientación al negocio. Aplicar un único marco de trabajo integrado. COBIT cubre todas las necesidades y se integra con otros marcos y buenas prácticas, de forma que puede ser utilizado como marco general. Aproximación holística. Para conseguir una Gestión y Gobierno de las TI con eficiencia y eficacia. Separar Gestión de Gobierno. Ambas disciplinas son importantes y complementarias.[15]

Grafico 1.7

Evolución del Cobit



En el anexo 3 se pone el modelo de referencia de procesos, y también la comparación de los modelos de madurez de la versión 4.1 y la versión 5.0

Capitulo 2

2. SITUACIÓN ACTUAL

La Universidad Politécnica Salesiana es una universidad ecuatoriana perteneciente a la congregación Salesiana, la Presencia salesiana en el campo universitario es relativamente nueva, salvo las experiencias educativas de la India en 1934 y la Pontificia Universidad Salesiana que forma a los salesianos en la educación superior desde 1940 en Turín, inicialmente como Pontificio Ateneo Salesiano y desde 1973 como Universidad con sede en Roma. En la actualidad existen 35 inspectorías Salesianas con responsabilidad de Educación Superior, lo que implica un crecimiento muy alto de la oferta universitaria salesiana en el mundo.

MISIÓN: La formación de honrados ciudadanos y buenos cristianos, con excelencia humana y académica. El desafío de nuestra propuesta educativa liberadora es formar actores sociales y políticos con una visión crítica de la realidad, socialmente responsables, con voluntad transformadora y dirigida de manera preferencial a los pobres.

VISIÓN: La Universidad Politécnica Salesiana, inspirada en la fe cristiana, aspira constituirse en una institución educativa de referencia en la búsqueda de la verdad, el desarrollo de la cultura, de la ciencia y tecnología, mediante la aplicación de un estilo educativo centrado en el aprendizaje, docencia, investigación y vinculación con la colectividad, por lo que se compromete, decididamente, en la construcción de una sociedad democrática, justa, equitativa, solidaria, con responsabilidad ambiental, participativa y de paz.

RESEÑA HISTORICA: La presencia Salesiana en el Ecuador es una realidad social desde enero de 1888, como respuesta al Convenio firmado por Don Bosco y el representante del Gobierno del Ecuador en Turín (Italia) en 1887, por el que se confía a los salesianos el Protectorado Católico de Artes y Oficios de Quito, para que "*impartan educación moral y científica a los hijos del pueblo y para el desarrollo de la industria nacional mediante una enseñanza sistemática de la artesanía*"

Muy pronto la obra evangélica-educativa de los salesianos se extendió a otras ciudades del Ecuador, destacándose entre las principales acciones la fundación de las Misiones en el Oriente Ecuatoriano como Gualaquiza (1893), Indanza (1914), Méndez (1915), Macas (1924), Sucúa (1931) y Limón (1936).

La Educación Universitaria

El 4 de agosto de 1994, el Presidente de la República del Ecuador, Arquitecto Sixto Durán Ballén firma el decreto presidencial de creación de la UPS y nace nuestra Institución en la sociedad ecuatoriana en una época muy crítica desde el punto de vista social y económico, cuyo resultado es la extrema pobreza, que trae aparejada una secuela de descomposición social y moral.
Una vez aprobado el Proyecto de creación de nuestra Universidad, la Sociedad Salesiana del Ecuador resuelve iniciar las actividades del nuevo Centro de Educación Superior, en el mes de octubre de 1994. Previamente el septiembre 6 de 1994 se instala el primer Consejo Universitario y se realiza la posesión del Rector y Vicerrector y nace oficialmente la Universidad Politécnica Salesiana como centro de educación superior.

Objetivos

- Educar en la fraternidad a los jóvenes ecuatorianos para la promoción total de sus personas, ofreciéndoles una propuesta que parte de la acogida de sus valores propios y el llamamiento a la solidaridad, en el contexto de la comunidad social y eclesial.
- Formar personas con madurez humana que sepan hacer coherentemente la síntesis de ética, vida y cultura, para que actúen en la historia en la línea de la justicia, solidaridad y fraternidad, testimoniando los valores éticos más altos del hombre.
- Intensificar la conformación de comunidades educativas para desarrollar una educación en perspectivas de liberación, que forme a los jóvenes en valores, en el conocimiento, en el trabajo y en la participación social.
- Promover el desarrollo de cambios cualitativos en la educación que ofrecen los centros salesianos, con miras a establecer modelos pedagógicos alternativos que satisfagan las necesidades de los aprendizajes que favorecen la vida personal y social en sus dimensiones auténticas.

2.1 Descripción de la organización administrativa de la UPS Guayaquil

La estructura organizativa está centralizada en la sede cuenca con el rector actualmente presidido por el padre Javier Gómez al frente de la organización seguido del vicerrector general, el vicerrector académico y los diferentes Vicerrectores de cada sede: Cuenca, Guayaquil y Quito. Para manejar de una mejor forma todas las carreras, se dividieron en 4 secciones:

- Áreas del Conocimiento
- Unidades Académicas
- Departamentos de Apoyo
- Secretarias Técnicas

Dentro de los especialistas a nivel de Aéreas del conocimiento todas las sedes: Educación, Humanidades, Razón y fe, Ciencias Sociales y del comportamiento Humano, Administración y Economía, Ciencias Exactas, Ciencia y Tecnología, Ciencias Agronómicas y veterinaria y Ciencias de la vida.

En las unidades académicas están divididos en Educación a distancia y virtual, Posgrados, Investigación, Vinculación, Planeación Evaluación y Acreditación.

En los departamentos de apoyo se encuentran: Secretario General-Procurador, Auditoria, Contadora General.

Y por ultimo y no menos importante las secretarias técnicas: Bienestar Estudiantil, Gestión del talento humano, Presupuesto y Finanzas, Comunicación, Tecnologías de la Información, Estadística, Construcciones.

A continuación se presenta el diagrama organizacional de la universidad:

GRAFICO 2.1 DIAGRAMA ORGANIZACIONAL DE LA UPS

Fuente: Universidad Politécnica Salesiana

Una vez que detallamos

- **Funciones del Departamento de Sistemas**

Servicios para la docencia

Las áreas de TI deben asegurar a los estudiantes y docentes de la Universidad el uso confiable de los equipos de TI. Brindara asistencia técnica en la adquisición de hardware y software que ayuden al desenvolvimiento de la academia.

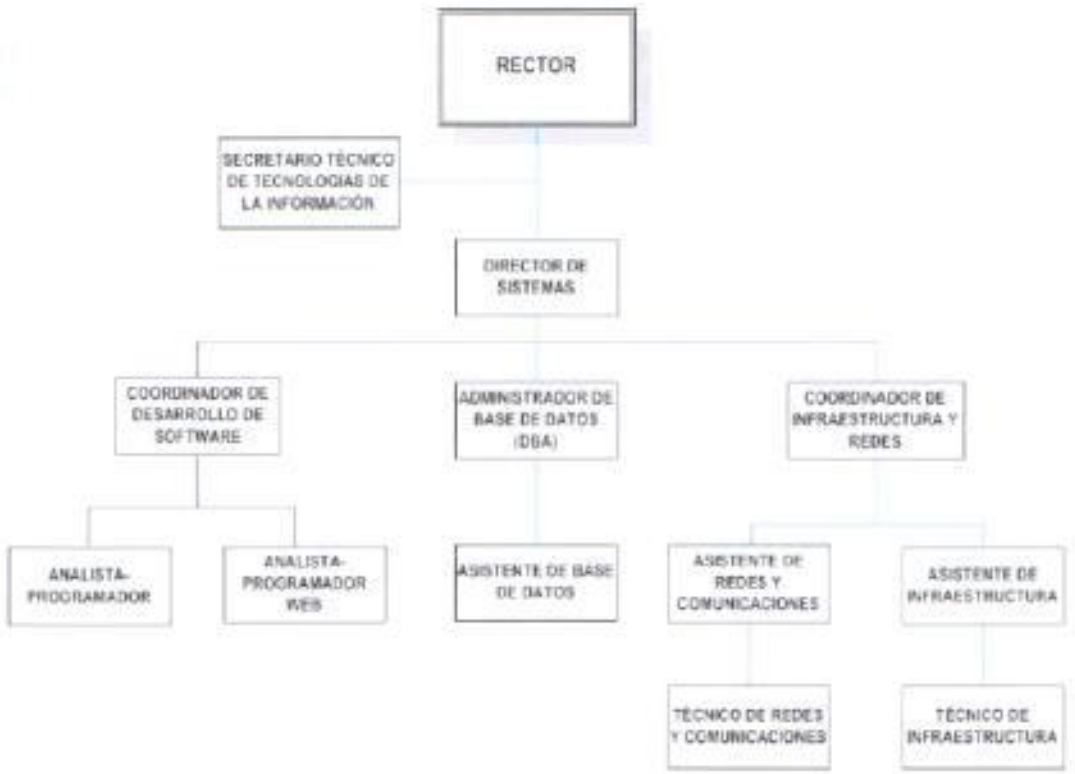
Servicios para la administración

Las áreas de TI, una vez recibido los requerimientos de las diferentes aéreas académicas o administrativas; analizarán, diseñarán y desarrollarán los programas necesarios para la gestión.

Servicios institucionales

Los departamentos de TI deberán promover la automatización de los servicios académicos y administrativos de la UPS, así como el uso de las tecnologías de información y comunicación.[14]

GRAFICO 2.2 ESTRUCTURA ORGÁNICA FUNCIONAL Y DE RESPONSABILIDADES DEL ÁREA DE TI - RECTORADO

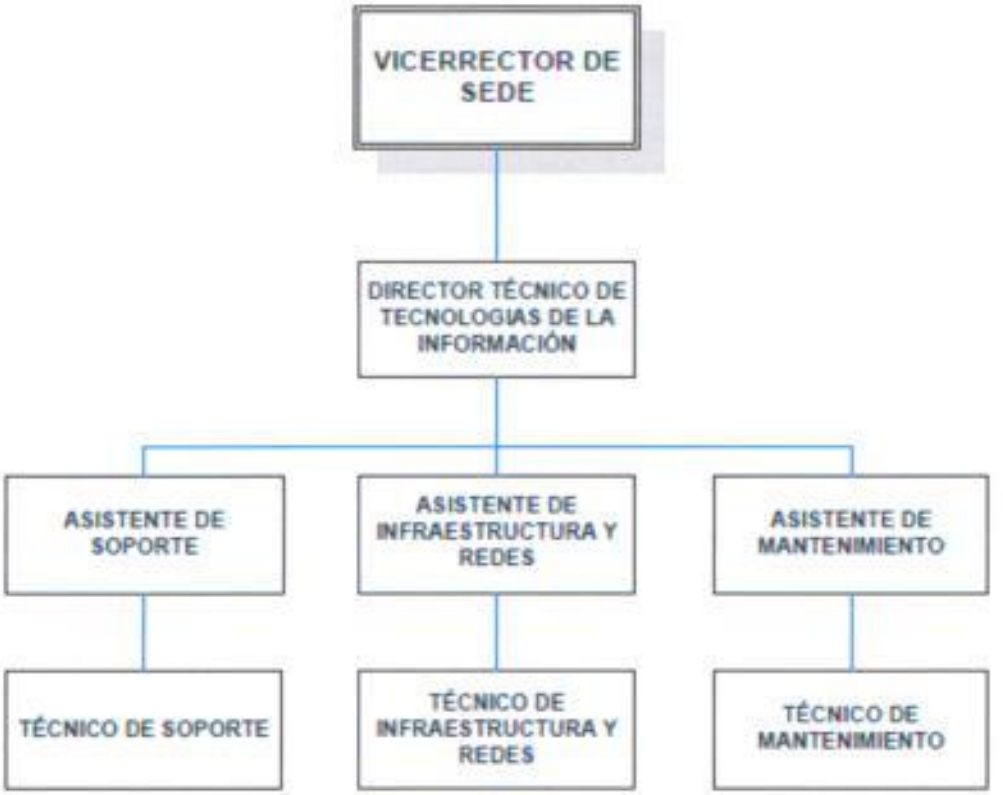


Personal Actual de Rectorado:

Cargo	Nombre
Secretario Técnico de Tecnologías de Información.	Ing. Juan Vicuña
Director de Sistemas	Analista. Fernando Narvaez
Coordinador de Desarrollo de Software	
Administrador de Base de datos	Ing. Edison Quintuña
Coordinador de Infraestructura y Redes	Ing. Patricio Jimenez

Analista - Programador	Ing. Jesica Zuñiga Ing. Jesica Cambi Ing. Andrea Jara
Analista – Programador Web	Ing. Andrés Urgiles Ing. Fernando Cevallos
Asistente de Base de datos	Ing. Jenifer Yepez
Asistente de Redes y Comunicaciones	Ing. Sandro Santander
Administrador de Infraestructura y Redes	Ing. Marco Timbi
Asistente de Redes y Comunicaciones	
Asistente de Infraestructura	

GRAFICO 2.3 ESTRUCTURA ORGÁNICA FUNCIONAL Y DE RESPONSABILIDADES DEL ÁREA DE TI - SEDES



Personal actual por Sedes

Sede Cuenca

Cargo	Nombre
Coordinador de Tecnologias de Información	Ing. Giovanni Sagbay
Asistente de Mantenimiento	Ing. Juan Carlos Proaño
Asistente de Infraestructura y Redes	
Asistente de Mantenimiento	Ing. Patricio Ortiz
Técnico de Soporte	
Técnico de Infraestructura y Redes	
Técnico de Mantenimiento	

Sede Quito

Cargo	Nombre
Coordinador de Tecnologias de Información	Ing. Alberto Duchi
Asistente de Mantenimiento	Ing. Klever Curay
Asistente de Infraestructura y Redes	Ing. Juan Carlos Dominguez
Asistente de Mantenimiento	
Técnico de Soporte	Tngl. Nancy Cali
Técnico de Infraestructura y Redes	
Técnico de Mantenimiento	Tngl. Francisco Baca Ángel Gualotuña Mayra Martínez Tngl. Patricia Tasintuña Diego Villegas

Sede Guayaquil

Cargo	Nombre
Coordinador de Tecnologias de Información	Ing. Javier Ortiz
Asistente de Mantenimiento	Ing. Martha Yanqui
Asistente de Infraestructura y Redes	Carlos Lucas
Asistente de Mantenimiento	Ing. Ricardo Mora
Técnico de Soporte	
Técnico de Infraestructura y Redes	Gabriel Tigua
Técnico de Mantenimiento	

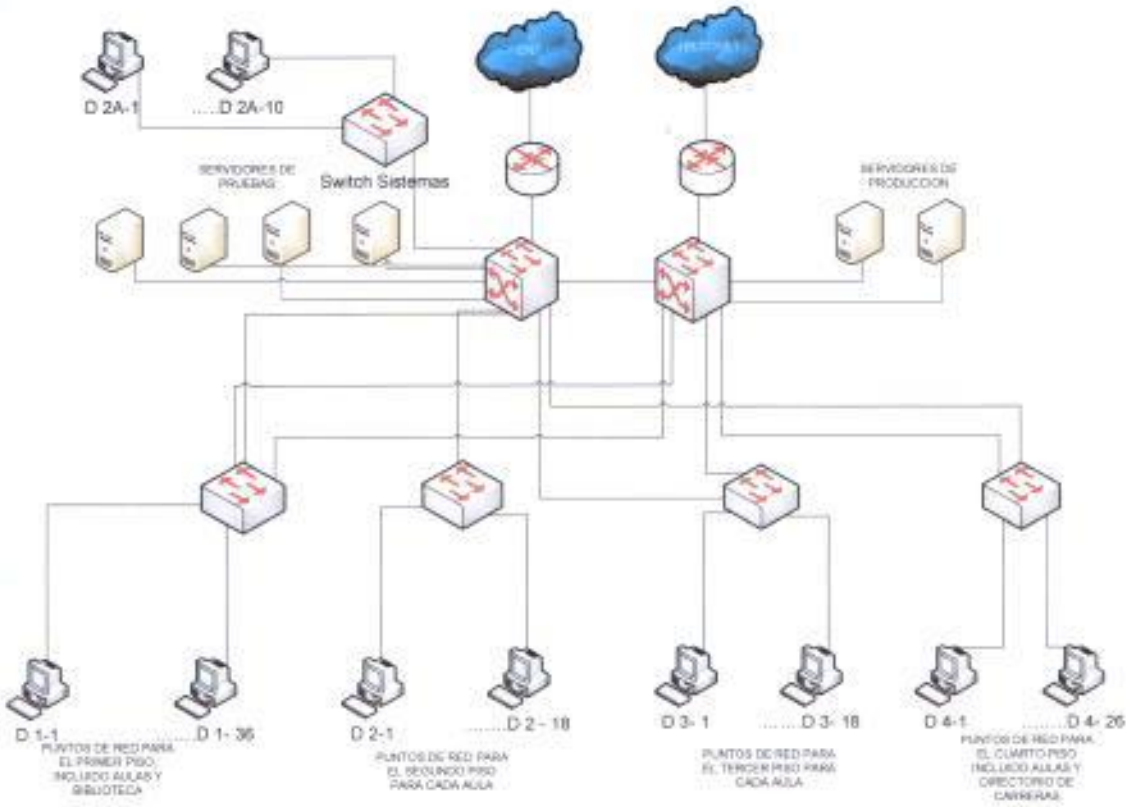
2.2 Infraestructura actual de la red informática de la UPS

La red informática de la empresa tiene como tecnología Ethernet, el cableado es estructurado categoría 6 en los tres edificios que conforman la sede Bloque B, D y la Joya, siendo el de mayor relevancia el edificio nuevo llamado Bloque D, en donde se aloja la infraestructura principal de la sede conjuntamente con el departamento de sistemas, y la unidad de bienestar estudiantil, aparte de ser sede de algunos departamentos como el Directorio de Carrera, el Departamento de Idiomas y la UNADEDVI que se encarga del correcto funcionamiento del AVAC, sistema que sirve para la comunicación con el estudiante y repositorio del material para las diferentes asignaturas.

A parte existe una infraestructura wireless que esta implementada en todo el campus filtrado por un proxy ubicado en el departamento de sistemas.

Grafico 2.4

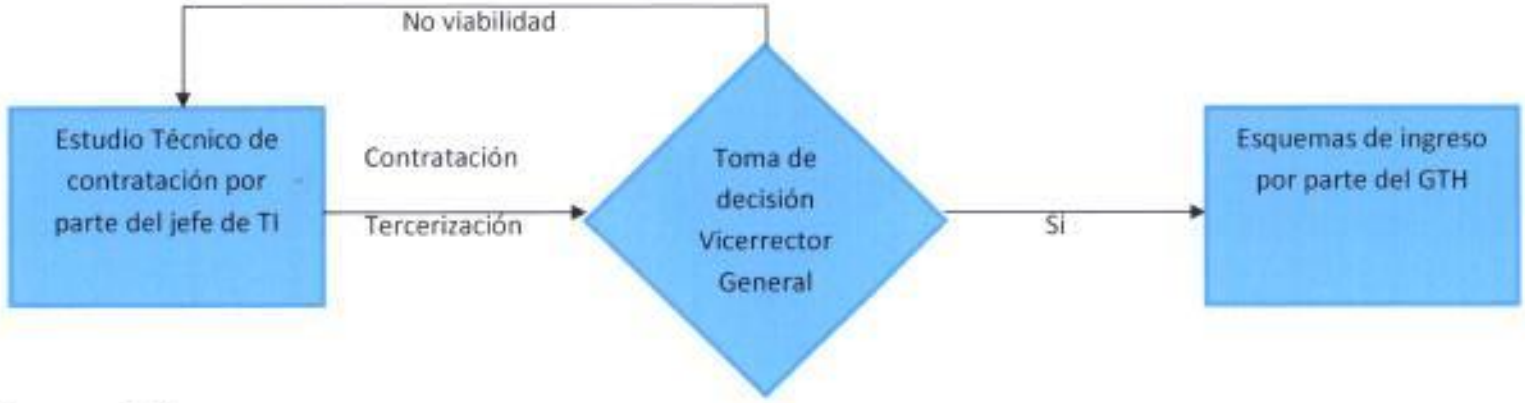
Diseño de la Red LAN edificio donde se aloja el Departamento de Sistemas



Por políticas de seguridad solo se presenta en el diseño los aspectos más fundamentales y necesarios de este.

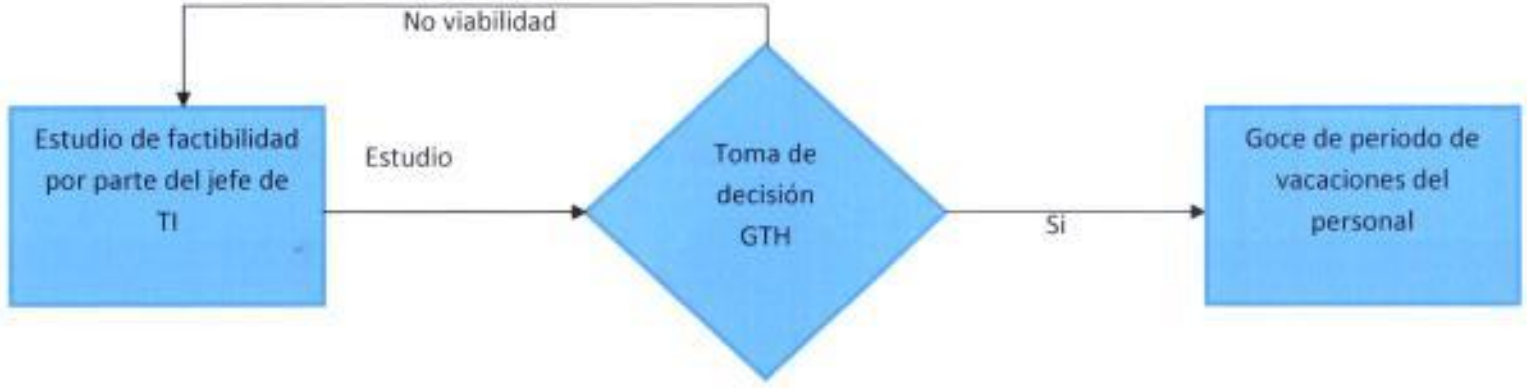
Grafico 2.5 Procesos

Contrataciones: Nuevo Personal T.I.

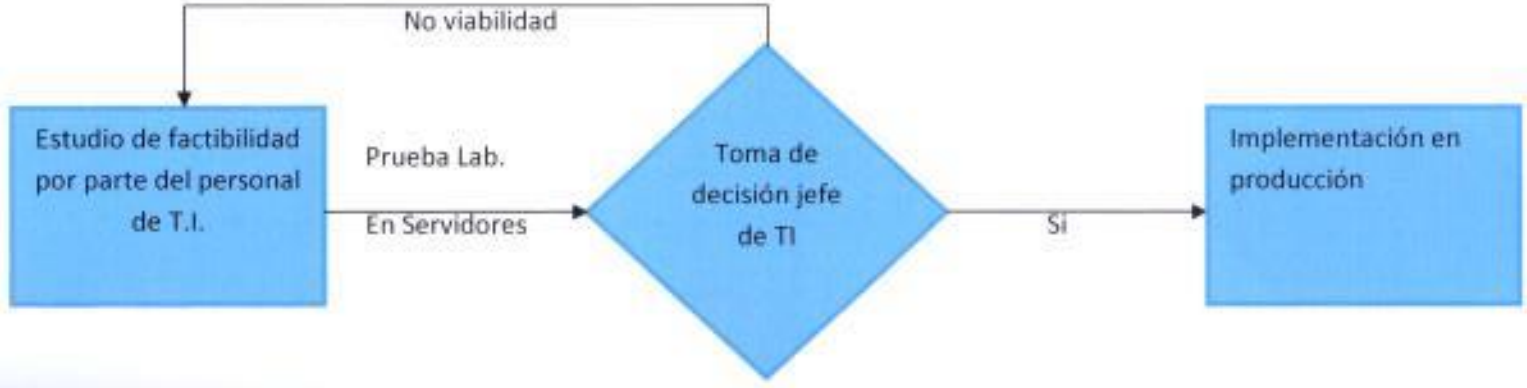


Compras T.I.

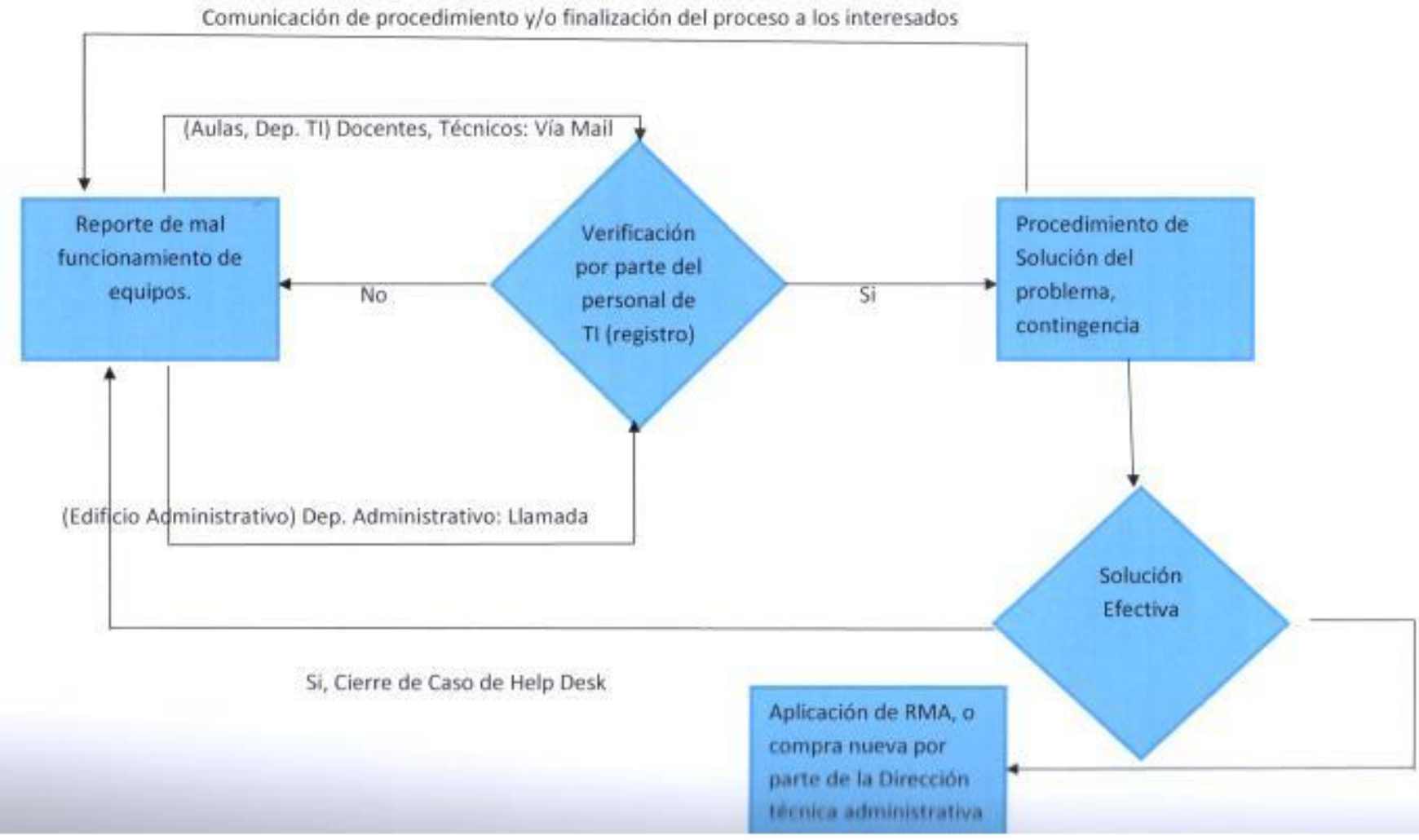
Contrataciones: Vacaciones Personal T.I.



Pruebas: Validación / Implementación / Mejoras



HelpDesk: Reparación



2.3 Evaluación de riesgos de la gestión de seguridad en la red del departamento de sistemas de la Universidad Politécnica Salesiana sede Guayaquil

Cobit se sustenta en varias fuentes para la definición de su estándar, tales como normas, estándares y programas que cuentan con auspicio del gobierno de los Estados Unidos, entre ellos el Instituto de Estándares y Tecnología (NIST), del cual se tomara uno de los documentos emitidos como base para la realización del Análisis de Riesgos.

Metodología NIST800-30 para administración de riesgos

La gestión de riesgos es el proceso de identificar, evaluar y ejecutar acciones para reducir el riesgo a un nivel aceptable.

El instituto de Estándares y Tecnología (NIST) libero su publicación especial 800-30 así como su actualización 800-30 revision 1 con recomendaciones para la administración de riesgo para los sistemas de información del cual se tomara los nueve pasos sugeridos para una correcta evaluación de riesgos. Estos son:

- Caracterización del Sistema
- Identificación de la Amenaza.
- Identificación de Vulnerabilidad.
- Análisis del Control.
- Determinación de Probabilidad.
- Análisis del Impacto
- Determinación del Riesgo
- Recomendaciones de los Controles
- Documentación de los Resultados.

Evaluación de Riesgos de la Gestión de la seguridad en la red del departamento de sistemas de UPS Guayaquil

- **Caracterización del Sistema**

De la determinación de los atributos de un sistema de TI se identifica el alcance de la evaluación del riesgo, las fronteras del sistema de TI, los recursos y la información que representa y conforma el sistema.

- **Identificación de Recursos de TI**

- **Recursos de hardware**

Marca, Modelo	Serial
IBM Systems x 3500 M3, MT:7380	KQ34NY9
IBM Total Storage, MT:3580-L4S	6S-P2291
IBM Blade Center H, MT: 8852	KQTNBZ4
Cisco Catalyst 4507K	FOX101112EX
Cisco Aironet	F0C1243J0SX
Cisco Aironet	F0C1243J070
Cisco Aironet	F0C1243J09W
Cisco Aironet	F0C1243J2VY
Cisco Aironet	F0C1243J0SW
Cisco 800	VAMKB00ARB
Cisco 3800	FTX1012A4AJ
Cisco ASA 5520 SSM-20	JMX1017K05D
Cisco Catalyst 3560	FD0120245JA
Cisco Catalyst 3560	FD01211X49S
KVM D-Link	BS0P2A100078
Cisco MCS7800	KQWPHGT
HP Proliant ML150 G	N/A
Clon PC	CP03TST06
Clon PC	CA04G7A07
Clon PC	CQ16GBC15

Enlace Última Milla Telconet 6 Mbps
Enlace Última Milla CNT 2 Mbps

- **Recursos de software**

Sistemas Operativos:

Microsoft Windows 2008 Server
Microsoft Windows XP
Microsoft Windows 7
Linux Centos
Linux Ubuntu
VmWare Server

Antivirus:
ESET NOD 32 (Corporativo)

Otro Software:
Microsoft Office 2010
Microsoft Office 2007

Aplicaciones:

Sistema Académico (SNA)
Sistema Financiero (SIA)
SQUAD (Nomina y Gestión Humana)
Oficina de Correos de Microsoft (Tercerizado)
Marcaciones
Sistema de Seguridad Panasonic

En los servidores se encuentra:

Firewall web Caching proxy con filtro de contenido
Application Control (P2P)
Antivirus Centralizado
DNS
FTP Server
LDAP
IDS/IPS (Cisco ASA 5520)
DHCP
SNMP
Active Directory
VPN (IPsec and PPTP)
Control de Ancho de Banda (QoS)
Web Server.

MEDIO OPERACIONAL DEL SISTEMA DE TI

Usuarios del Sistema

Los usuarios en el sistema son creados bajo demanda formal y por escrito, con autorización del jefe departamental y del jefe de recursos humanos, con perfiles definidos y accesos restringidos en cada uno de los servidores de acuerdo a las aplicaciones que usarán.

Políticas de seguridad del Sistema

No existe un manual de políticas de seguridad que describa el uso de los recursos de hardware, software, aplicaciones, e-mail y acceso a Internet. Pero se da a conocer a todos los empleados cuyas labores se relacionen con el uso de los recursos mencionados el momento de su incorporación a la universidad ciertos lineamientos de seguridad básicos.

Ambiente de seguridad Físico

La universidad cuenta con seguridad privada distribuida por todo el perímetro de la universidad, incluido el departamento de Sistemas se encuentra en una parte anexa a las aulas, cerca del departamento denominado Pastoral o centro de razón y fe, cuenta con un control de acceso mediante tarjetas magnéticas y las únicas personas autorizadas para el ingreso son el personal de Sistemas.
A parte de eso no existe un registro de quien ingresa al departamento salvo video de cámara ip con almacenamiento limitado.

Medioambiente de sistema TI

El grupo de servidores se encuentra ubicado en un cuarto de equipos (centro de datos) dentro del Área de Sistemas el cual cuenta con un sistema de aire acondicionado para el control de temperatura, sistemas de detección de incendios y un extintor manual.
El Área de Sistemas no se encuentra expuesta a la humedad o inundaciones por su ubicación física en el edificio.
En lo que se refiere a las computadoras personales todas cuentan con sistema de reguladores de voltaje y UPS.

Técnicas de Recolección de Información

La recolección de información se sustentó en los siguientes materiales y procedimientos aplicados:

- Entrevista al jefe del departamento de Sistemas.
- Revisión de manuales de procedimientos, planes de contingencia, contratos con terceros, inventarios de hardware y software.
- Observación del sitio.

Identificación de Amenazas

Previamente, se tendrán claramente definidos los conceptos de:

Amenaza: Posibilidad de ejercer de forma accidental o intencional una vulnerabilidad.

Vulnerabilidad: Debilidad que puede ser accidental o intencionalmente explotada.
Así, las posibles amenazas identificadas dentro de la red de datos del departamento de sistemas de la UPS son:

Amenazas naturales

Terremoto
Erupciones volcánicas
Tormentas eléctricas
Inundaciones

Amenazas humanas

Acciones no intencionales como: Ingreso inadvertido de datos, mal uso de recursos.
Acciones deliberadas como: ataques a la red, carga de software malicioso, acceso no autorizado a información confidencial.

Amenazas Medioambientales

Falla en el Servicio de Energía
Falla en el Sistema de Comunicaciones
Falla de equipos y aplicaciones

Identificación de Vulnerabilidades

- El documento de políticas de TI no cuenta con un proceso de revisión definido.
- Falta de documentación específica de políticas de seguridad de TI.
- Falta de políticas de requerimientos de seguridad en contratos con terceros.

- Falta de un plan de clasificación de información o en su lugar una pauta que tome parte en la determinación de cómo la información debe ser manipulada y protegida.
- Falta de acuerdo de confidencialidad o de no revelación de la información como parte de los términos y condiciones iniciales del empleo para el personal.
- Falta de procedimiento formal para reportar los incidentes de seguridad por los canales de administración apropiados tan pronto como sea posible.
- Falta de procedimiento para verificar todos los boletines de advertencia e informativos con respecto al uso de software malicioso.
- Los medios de respaldo y los procedimientos para su restauración no están guardados en un lugar seguro y lejos del sitio actual.
- Falta de un procedimiento para el monitoreo y control del uso de los recursos de TI por parte los empleados.
- Falta de procedimiento de actualización de planes de contingencia.
- Falta de documentación formal para el registro de la entrega o retiro de recursos de TI al personal.
- Falta de contingencia para el fallo de equipos (servidores y de red) críticos.
- Falta de un procedimiento de revisión periódica de archivos logs de los servidores.
- Cuentas de usuario vigentes para personal que dejó de laborar en la empresa.
- Los usuarios no guardan confidencialidad de sus cuentas y passwords.

Probabilidad de Impacto de la Amenaza

Para la definición de la probabilidad que una amenaza afecte a una vulnerabilidad se tomó como referencia la tabla de la NIST:

Cuadro 2.1

Definición de Probabilidades

Nivel de Probabilidad	Ponderación	Definición
Alto	3	El origen de amenaza tiene alta motivación y suficientemente capaz, y los controles para

		prevenir que se ejerza la vulnerabilidad son ineficaces.
Medio	2	El origen de amenaza es motivado y capaz, pero los controles presentes pueden impedir que se ejerza con éxito la vulnerabilidad.
Bajo	1	El origen de amenaza carece de motivación o capacidad, existen controles para prevenir o por lo menos para impedir significativamente que se ejerza la vulnerabilidad.

De igual manera para la definición del impacto se consideró la tabla proporcionada por la NIST que define la magnitud del impacto en niveles alto, medio y bajo. Cabe notar que para la definición de estos niveles se toma en cuenta los siguientes criterios de seguridad: integridad, disponibilidad y confidencialidad.[2]

Cuadro 2.2

Definición de la magnitud del impacto

La magnitud del impacto	Ponderación	Definición
Alto	3	(1) puede producir la pérdida costosa de recursos; (2) puede dañar significativamente o impedir una misión de la organización, su reputación o intereses; o (3) puede resultar muerte o la lesión seria del personal.
Medio	2	(1) puede producir la pérdida costosa de activos tangibles o recursos; (2) puede dañar, o puede impedir la misión de la organización, su reputación o intereses; o (3) puede resultar en lesión del personal.
Bajo	1	(1) puede producir la pérdida de algunos recursos tangibles o recursos o (2) puede afectar notablemente la misión de la organización, su reputación, o intereses.

Determinación del Riesgo

La siguiente matriz se obtiene del producto entre los niveles de Probabilidad e Impacto definidos anteriormente, para conocer el riesgo que se aplica a la amenaza:

Cuadro 2.3

Matriz de ponderación

Probabilidad de la Amenaza	Impacto de la Amenaza		
	Bajo (1)	Medio (2)	Alto (3)
Alto	Bajo 3*1=3	Medio 3*2=6	Alto 3*3=9
Medio	Bajo 2*1=2	Medio 2*2=6	Alto 3*3=6
Bajo	Bajo 1*1=1	Medio 1*2=6	Alto 1*3=3

Resultado de la evaluación del riesgo

A continuación se presenta la Matriz de Evaluación de Riesgos, en donde se analizan cada uno de los recursos identificados considerados críticos, para cada uno de ellos se reconocen amenazas y vulnerabilidades, el control existente, su posible impacto y probabilidad de ocurrencia se reconoce a partir de la entrevista con los encargados de T.I y del checklist aplicado (Ver Anexo 2), el nivel de riesgo se obtiene de la aplicación de la matriz de ponderación anterior y finalmente se proponen las recomendaciones necesarias para alcanzar un control considerable.

Cuadro 2.4
Matriz de Evaluación de Riesgo

Recurso	Amenaza	Vulnerabilidad	Control Existente	Impacto	Probabilidad	Nivel de Riesgo	Recomendación
Servidores y PC	Mal uso de recursos	El documento de políticas de TI no cuenta con un proceso de revisión definido.	No existe un documento formal de políticas	Bajo	Medio	Bajo	Establecer las políticas mediante un documento, y un procedimiento para su actualización periódica
	Acceso no autorizado a información confidencial	El documento de políticas de TI no cuenta con un proceso de revisión definido.	No existe un documento formal de políticas	Bajo	Medio	Bajo	Establecer las políticas mediante un documento, y un procedimiento para su actualización periódica
	Mal uso de recursos y acceso no autorizado	El documento de políticas de TI no cuenta con un proceso de revisión definido.	No existe un documento formal de políticas de seguridad	Alto	Medio	Medio	Definir un documento de políticas de seguridad
	Acceso no autorizado a información confidencial	No existe una política de requerimientos de seguridad en contratos con	No existe un documento formal de políticas de	Alto	Medio	Medio	Añadir cláusulas de confidencialidad de la información en los contratos establecidos con

		terceros.	seguridad				compañías externas.
Servidores	Ataque a la red	No existe un procedimiento formal para reportar los incidentes de seguridad por los canales de administración apropiados tan pronto como sea posible.	Reportes informales.	Alto	Bajo	Bajo	Establecer un procedimiento de formal para reportar incidentes de seguridad.
	Acceso no autorizado a información confidencial	No existe un procedimiento formal para reportar los incidentes de seguridad por los canales de administración apropiados tan pronto como sea posible.	Reportes informales.	Alto	Medio	Medio	Establecer un procedimiento de formal para reportar incidentes de seguridad.
	Ataque a la red, mal uso de recursos y carga de	Falta de un procedimiento de revisión periódica de archivos logs de los servidores.	Ninguno	Bajo	Bajo	Bajo	Definir un procedimiento para la revisión periódica

	software malicioso						de los logs.
	Terremoto, Tormentas Eléctricas y Erupciones Volcánicas	Falta de un procedimiento de actualización de planes de contingencia	Plan de contingencia no actualizado y que no contempla amenazas naturales.	Alto	Medio	Medio	Establecer un plan de contingencia que contemple este tipo de amenazas.
Equipos de conexión de red	Mal uso de recursos	El documento de políticas de TI no cuenta con un proceso de revisión definido.	No existe un documento formal de políticas	Medio	Medio	Medio	Establecer las políticas mediante un documento, y un procedimiento para su actualización periódica
	Ataque a la red y mal uso de recursos	Falta de un procedimiento formal para reportar los incidentes de seguridad por los canales de administración apropiados tan pronto como sea posible.	Reportes informales.	Alto	Bajo	Bajo	Establecer un procedimiento de formal para reportar incidentes de seguridad.
	Terremoto, Tormentas Eléctricas y	Falta de un procedimiento de actualización de	Plan de contingencia no actualizado	Alto	Medio	Medio	Establecer un plan de contingencia que contemple este tipo

	Erupciones Volcánicas	planes de contingencia	y que no contempla amenazas naturales.				de amenazas.
PC	Carga de software malicioso	No existe un procedimiento para verificar todos los boletines de advertencia e informativos con respecto al uso de software malicioso.	Se define usuarios con perfil limitado para cada caso.	Bajo	Medio	Bajo	Verificar periódicamente los boletines y dar a conocer a los usuarios.
	Mal uso de recursos	No existe un procedimiento para el monitoreo y control del uso de los recursos de TI por parte los empleados.	Reportes Informales	Bajo	Alto	Bajo	Establecer las políticas mediante un documento, y un procedimiento para monitorear el uso de los recursos de TI
	Terremoto, Tormentas Eléctricas y Erupciones Volcánicas	Falta de un procedimiento de actualización de planes de contingencia	Plan de contingencia no actualizado y que no contempla amenazas naturales.	Alto	Medio	Medio	Establecer un plan de contingencia que contemple este tipo de amenazas.
Correo	Mal uso de	No existe un					Definir nuevas

Electrón ico	recursos	procedimiento formal para el monitoreo y control del uso del recurso	Reportes Informales	Medio	Alto	Medio	políticas sobre uso de correo, negar envío de cadenas, rios de información no laboral, posible fuente de virus y pérdida de datos.
Sistema de UPS	Falla en servicio de energía	No existe un procedimiento de actualización de planes de contingencia.	Contingencia establecida, pero no documentada	Alto	Medio	Alto	Establecer las políticas mediante un documento, y un procedimiento para la contingencia eléctrica.
Enlaces de Ultima Milla	Acceso no autorizado a información confidencial	No existe una política de requerimientos de seguridad en contratos con terceros.	Ninguno	Alto	Medio	Medio	Añadir cláusulas de confidencialidad de la información en los contratos establecidos con compañías externas.
	Ataque a la red y mal uso de recursos	No existe un procedimiento formal para reportar los incidentes de seguridad por los canales de administración apropiados tan	Reportes Informales	Alto	Bajo	Bajo	Establecer un procedimiento de formal para reportar incidentes de seguridad.

		pronto como sea posible.					
Aplicaciones en red SNA, SIA, SQUAD	Ingreso inadvertido de datos	Definición o asignación errónea de perfiles de usuario.	Documento de solicitud de creación de la cuenta de usuario.	Alto	Bajo	Bajo	Revisión periódica de las cuentas existentes y sus perfiles.
		Cuentas de usuario vigentes para personal que dejó de laborar en la empresa.	Reporte del Área de Recursos Humanos de los empleados salientes.	Alto	Bajo	Bajo	El reporte emitido por Recursos Humanos del personal saliente debe ser periódico.
	Acceso no autorizado a información confidencial	Los usuarios no guardan confidencialidad de sus cuentas y passwords.	Los usuarios conocen su responsabilidad sobre la no divulgación de sus cuentas.	Alto	Bajo	Bajo	Reforzar la conciencia de responsabilidad de los usuarios sobre el uso de sus cuentas.
	Ingreso de datos erróneos que produzcan información no confiable	El buen funcionamiento del sistema de contabilidad depende en gran medida de los datos recogidos de los sistemas de nomina, inventario y del	Cierre periódicos de cada uno de los sistemas involucrados antes de pasar al Sistema de Contabilidad.	Alto	Bajo	Bajo	Mantener el procedimiento de cierres periódicos de los sistemas.

		proceso de auditoría diario.					
	Mal uso de recursos y acceso no autorizado	Falta un plan de clasificación de información o una pauta que tome parte en la determinación de cómo la información debe ser manipulada y protegida.	La información considerada clave para un usuario es almacenada en el servidor, con controles de acceso restringido.	Alto	Medio	Medio	Elaborar el plan de clasificación de la información y dar a conocer a los involucrados.
		Falta de un acuerdo de confidencialidad o de no revelación de la información como parte de los términos y condiciones iniciales del empleo para el personal.	Ninguno	Medio	Alto	Medio	Elaborar un acuerdo de confidencialidad que sea parte de contrato de empleo.
	Ataque a la red	Falta de un procedimiento de actualización de planes de contingencia.	Plan de contingencia no formalizado ni actualizado	Alto	Medio	Medio	Establecer un plan de contingencia que contemple este tipo de amenazas.

Servicio de Internet	Mal uso de recursos	Falta de un procedimiento para el monitoreo y control del uso de los recursos de TI por parte los empleados.	Política actual del uso de TI y Control de consumo del ancho de banda en Servidor Proxy	Medio	Alto	Medio	Definir un procedimiento para monitorear el uso de los recursos de TI.
	Falla en el sistema de comunicaciones	Falta de un procedimiento de actualización de planes de contingencia.	Contingencia establecida pero no documentada	Alto	Bajo	Bajo	Establecer un plan de contingencia que contemple este tipo de amenazas.
	Terremoto, Tormentas Eléctricas y Erupciones Volcánicas	Falta de un procedimiento de actualización de planes de contingencia.	Plan de contingencia no actualizado y que no contempla amenazas naturales.	Alto	Medio	Medio	Establecer un plan de contingencia que contemple este tipo de amenazas.

PLAN DE AUDITORIA PARA LA GESTION DE SEGURIDAD DE LA RED

2.4 Alcance de la auditoria de la gestión de seguridad.

El siguiente trabajo de auditoría aplicará COBIT como metodología para la evaluación y análisis de los diferentes procesos y controles que se aplican en el área de la tecnología de la información.

A pesar de que COBIT es una herramienta que trabaja conjuntamente con los objetivos principales de la organización, la auditoría se centrara en el análisis de la gestión de la seguridad informática que es aplicada actualmente en la red de datos del departamento de TI de la universidad Politécnica Salesiana sede Guayaquil

Debido a que UPS es una universidad privada dedicada exclusivamente a ofrecer los mejores servicios a sus estudiantes (pregrado – postgrado), todos los esfuerzos de la organización van encaminados a alcanzar esta meta sin dejar de lado el obtener importantes ingresos asegurando su posición creciente en el mercado manteniendo la fidelidad de sus clientes. Para llegar a este nivel de servicio; cada departamento unos en mayor proporción que otros deben asegurarse de dar lo mejor de sí, de que se identifican aquellos que para mantener en operación constante dependen del servicio que les brinda la red informática; estos son: Docentes, Dirección de carrera, Contabilidad, Pastoral, Ventas, Compras y Adquisiciones, Recursos Humanos y Sistemas.

De aquí partirá el análisis donde se identificaran las debilidades existentes y sus riesgos potenciales, se expondrán una serie de conclusiones sobre los actuales procedimientos y controles de seguridad así como recomendaciones para el mejoramiento de la gestión de seguridad.

OBJETIVOS DE LA AUDITORÍA

- Analizar y diagnosticar la actual gestión de seguridad en la red de datos de la UPS sede Guayaquil.

- Plantear las mejoras para la gestión de la seguridad de la red de datos.
- Proponer nuevos procesos y actividades que ayudaran a identificar los controles que se requieren para garantizar la seguridad de la información.

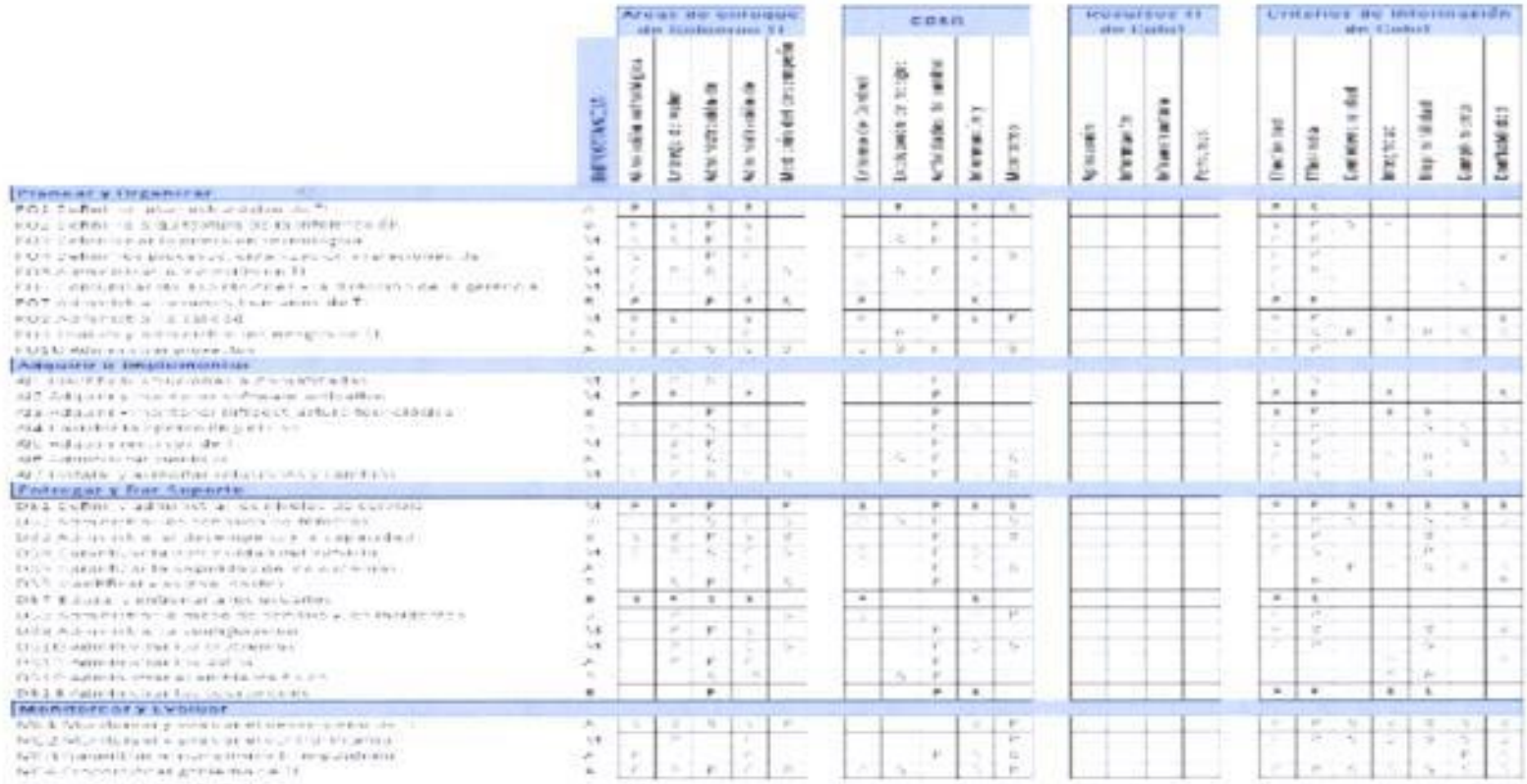
2.5 Determinación de los procesos COBIT aplicables a la gestión de seguridad.

La determinación de los procesos COBIT involucrados dentro de la gestión de seguridad en redes que permitirán llevar a cabo el desarrollo de la presente auditoría, fue realizada siguiendo las recomendaciones del documento Security Baseline de COBIT que fue publicado a inicios del 2008. Este documento expone los objetivos de control detallados de COBIT que tienen relación con la seguridad en un ambiente de T.I. Del estudio de estos, se han seleccionado aquellos que tienen relación con la gestión de la seguridad de la red informática que sean aplicables a la naturaleza del negocio y que contribuyen a alcanzar los objetivos del negocio.

A continuación se exponen los objetivos de control por dominios que han sido escogidos para la ejecución del trabajo de auditoría de la gestión de seguridad de la red informática.

P02 Definición de la Arquitectura de la Información
P04. Definición de los procesos, Organización y las relaciones de TI.
P06. Comunicación de las aspiraciones y la dirección de la Gerencia.
P07. Administrar los Recursos de TI
P09. Evaluación y administración de los riesgos de TI.
AI3. Adquisición y mantenimiento de la infraestructura tecnológica.
DS2. Administración de servicios prestados por terceros.
DS4. Garantizar la continuidad del servicio.
DS5. Garantizar la seguridad de Sistemas.
DS9. Administración de la Configuración.
DS11. Administración de Datos.
DS12. Administración del ambiente físico.
ME3. Garantizar el cumplimiento con Requerimientos Externos.

Cuadro 2.5 OBJETIVOS DE CONTROL COBIT – CRITERIOS Y RECURSOS TI AFECTADOS



(P=Primario, S=Secundario).

Fuente: Marco Referencial COBIT

DOMINIO: PLANEACION Y ORGANIZACIÓN

PO2 Definición de la arquitectura de la información

La función de sistemas de información debe crear y actualizar de forma regular un modelo de información del negocio y definir sistemas apropiados para optimizar el uso de esta información

Los objetivos de control detallados a ser considerados son:
PO 2.3 Esquema de clasificación de Datos.

PO4 Definición de los procesos, organización y las relaciones de TI

Para conocer si las responsabilidades de seguridad están definidas, entendidas y asignadas apropiadamente.

Los objetivos de control detallados a ser considerados son:
PO4.6 Establecimiento de Roles y Responsabilidades
PO4.11 Segregación de funciones

PO6 Comunicación de las aspiraciones y la dirección de la gerencia

Para que las políticas relacionadas con la seguridad de TI sean establecidas y se den a conocer al personal.

Los objetivos de control a ser considerados son:
PO6.4 Implantación de Políticas de TI
PO6.5 Comunicación de los objetivos y la dirección de TI

PO7 Administrar los Recursos Humanos de TI

Para asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y sean conscientes de los riesgos y responsabilidades involucrados.

Los objetivos de control detallados a ser considerados son:
PO7.4 Entrenamiento del Personal de TI

PO9 Evaluar y Administrar los Riesgos de TI

Identificar que puede ir mal con la seguridad de TI y su impacto en los objetivos del negocio, considerar como asegurar datos y transacciones que son críticos para el negocio, preparar un plan de acción para manejo de riesgos y concientizar al personal sobre los riesgos de seguridad.

Los objetivos de control detallados a ser considerados son:

PO 9.3 Identificación de Eventos..
PO 9.5 Respuesta a los Riesgos.

DOMINIO: ADQUISICION E IMPLEMENTACION

AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica

Se refiere a la seguridad apropiada para la infraestructura tecnológica (hardware y software) que tiene que ver con la actualización, mantenimiento y adquisición.

Los objetivos de control detallados a ser considerados son:

AI3.2 Protección y Disponibilidad del Recurso de infraestructura
AI3.3 Mantenimiento de la Infraestructura.

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE

DS2 Administración de Servicios Prestados por Terceros

Se refiere a la definición en cuanto a los aspectos de seguridad, confidencialidad y continuidad de los servicios prestados por terceros.

Los objetivos de control detallados a ser considerados son:

DS2.3 Administración de Riesgos del Proveedor

DS4 Garantizar la continuidad del Servicio

Se refiere a la capacidad de la empresa de seguir brindando el servicio contando con un plan de contingencias para la recuperación

de fallas después de incidentes en un tiempo mínimo y disponer de respaldos confiables. [7]

Los objetivos de control detallados a ser considerados son:

DS4.2 Planes de continuidad de TI.
DS4.5 Pruebas del plan de continuidad de TI.
DS4.8 Recuperación y reanudación de servicios de TI.
DS4.3 Recursos críticos de tecnología de información.
DS4.9 Almacenamiento de respaldo fuera de las instalaciones.

DS5 Garantizar la Seguridad de Sistemas

Contempla el control de acceso a sistemas para los diferentes usuarios, detectar, reportar y solucionar incidentes de violación de seguridad, protección de respaldos, etc.

Los objetivos de control detallados a ser considerados son:

DS5.1 Administración de la Seguridad de TI.
DS5.3 Administración de Identidad
DS5.4 Administración de cuentas de usuario.
DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad.
DS5.6 Definición de Incidente de Seguridad.
DS5.9 Prevención, detección y corrección de software malicioso.
DS5.10 Seguridad de la Red.
DS5.11 Intercambio de Datos Sensitivos

DS9 Administración de la Configuración

Tiene que ver con el mantenimiento actualizado de inventario de hardware y software sus licencias y configuraciones.

Los objetivos de control detallados a ser considerados son:

DS9.3 Revisión de Integridad de la Configuración.

DS11 Administración de Datos

Contempla la integridad y confiabilidad de los datos, estos deben ser accedidos solo por gente autorizada.

Los objetivos de control detallados a ser considerados son:

DS11.7 Chequeos de exactitud, suficiencia y autorización.

DS11.8 Manejo de Errores en la entrada de datos.
DS11.9 Integridad de procesamiento de datos.
DS11.10 Validación y Edición de procesamiento.
DS11.23 Respaldo y restauración.
DS11.24 Funciones de respaldo.
DS11.27 Protección de mensajes sensitivos.
DS11.29 Integridad de transacciones electrónicas.

DS12 Administración del Ambiente Físico

Seguridades físicas del área de Tecnología de información incluye cableado de red, equipos de comunicación, computadores, periféricos y electricidad.

Los objetivos de control detallados a ser considerados son:
DS12.2 Medidas de Seguridad Física.
DS12.4 Protección contra factores ambientales.
DS12.5 Administración de Instalaciones Físicas

DOMINIO: MONITOREO y EVALUACION

ME3 Garantizar el cumplimiento con requerimientos externos

Una supervisión efectiva del cumplimiento requiere del establecimiento de un proceso de revisión para garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales.

Los objetivos de control detallados a ser considerados son:
ME3.1 Identificar los requerimientos de las Leyes, Regulaciones y Cumplimientos contractuales.

En total se planea auditar, 13 Objetivos de Control generales y 44 detallados.

2.6 Herramientas aplicables al desarrollo de la auditoria.

Para poner en práctica el procedimiento de auditoría se gestionará la recolección de datos y documentación necesaria, además se tomarán como guías los siguientes documentos:

COBIT Security Baseline

COBIT Security Baseline transforma parte importante de los 34 objetivos de control de alto nivel de COBIT en 39 pasos para la seguridad de la información.
Abarca riesgos y precauciones de seguridad.

En base a este documento se filtraron los procesos u objetivos de control relacionados con la gestión de la seguridad de redes.

Directrices de Auditoria COBIT

Las Directrices de Auditoría servirán para verificar el cumplimiento de los objetivos de control detallados en base a posibles controles que deben aplicarse a cada objetivo y pruebas que evalúen su cumplimiento adecuado.

NIST Risk Management Guide for Information Technology Systems

Las recomendaciones emitidas por la NIST (National Institute of Standars and Technology) en su publicación 800-30 servirá como metodología para el análisis de riesgos e identificación de amenazas y vulnerabilidades.

2.7 Plan de auditoria

A continuación se presentan las principales actividades para realizar este trabajo de Auditoria:

1. Descripción de la Organización Administrativa
   - Infraestructura Actual de la Red.
   - Evaluación de Riesgos de la Gestión de Seguridad de la Red Informática.
2. Elaboración del Plan de Auditoria
   - Definición del alcance de la Auditoria.
   - Selección de los Procesos COBIT aplicables a la Auditoria.
3. Puesta en marcha del Plan de Auditoria
   - Elaboración del Programa de Auditoria.
   - Elaboración de Matriz de Pruebas.
   - Recolección de documentación: Manuales de procedimientos, funciones y politicas.
4. Evaluación y Análisis de las pruebas realizadas.
5. Elaboración del Informe Preliminar.
6. Elaboración del Informe Final.

La persona responsable de la realización de la auditoría es:
José R. Patiño Sánchez (Docente de la Universidad Politécnica Salesiana).
Javier Ortiz (Jefe del departamento de Sistemas de la UPS.

CAPÍTULO 3

3. PUESTA EN MARCHA DEL PLAN DE AUDITORÍA

El desarrollo del plan de auditoría se enfocará en la elaboración del programa de auditoría para cada uno de los objetivos de control detallado en el cual se determinará los factores de riesgo aplicados al objetivo en cuestión.
A partir de éste y tomando como base las Directrices de Auditoría COBIT se desarrollará la matriz de pruebas en la cual se definirán las pruebas específicas han ser aplicadas para determinar el cumplimiento del objetivo de control detallado.[12]

3.1 Procesos del Dominio de Planeación y Organización

Cuadro 3.1

Programa de Auditoria PO 2.3

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
PO 2 Definir la Arquitectura de la Información	
Establecer un sistema de clasificación de la información que se aplique a toda la empresa.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
PO 2.3 Esquema de Clasificación de datos La Jefatura deberá implementar procedimientos para asegurar que todos los datos son clasificados en términos de sensitividad, mediante una decisión explicita y formal del dueño de los datos de acuerdo con el esquema de clasificación de datos. Aún los datos que "no requieren protección" deberán contar con una decisión formal que les asigne dicha clasificación. Los dueños deben determinar la ubicación o disposición de sus datos y determinar quienes pueden compartir los datos aun si y cuando los programas y archivos sean mantenidos, archivados o borrados. Debe quedar evidencia de la aprobación del dueño y de la disposición del dato. Se deben definir políticas para soportar la reclasificación de la información, basados sobre cambios en la sensitividad. El esquema de clasificación debe incluir criterios para administrar el intercambio de información entre organizaciones, teniendo en cuenta tanto la seguridad y el cumplimiento como la legislación relevante.	□ Acceso a datos no definidos acorde a su criticidad los datos que no están bien clasificados no tienen un adecuado plan de recuperación. □ La política de T.I. no contempla la reclasificación de la información por su sensibilidad.

Cuadro 3.2

Matriz de pruebas PO 2.3

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
PO 2 Definir la Arquitectura de la Información		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO2.3 Esquema de Clasificación de datos La jefatura deberá implementar procedimientos para asegurar que todos los datos son clasificados en términos de sensitividad, mediante una decisión explícita y formal del dueño de los datos de acuerdo con el esquema de clasificación de datos. Aún los datos que "no requieren protección" deberán contar con una decisión formal que les asigne dicha clasificación. Los dueños deben determinar la ubicación o disposición de sus datos y determinar quienes pueden compartir los datos aun si y cuando los programas y archivos sean mantenidos, archivados o borrados.	*Evaluación de controles:* Se cuenta con un esquema de clasificación de datos en operación que indique que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido.	Revisión de manuales de procedimientos y funciones Entrevista al jefe de TI.

Cuadro 3.2 CONTINUACION

Matriz de pruebas PO 2.3

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
PO 2 Definir la Arquitectura de la Información		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO2.3 Esquema de Clasificación de datos Debe quedar evidencia de la aprobación del dueño y de la disposición del dato. Se deben definir políticas para soportar la reclasificación de la información, basados sobre cambios en la sensitividad. El esquema de clasificación debe incluir criterios para administrar el intercambio de información entre organizaciones, teniendo en cuenta tanto la seguridad y el cumplimiento como la legislación relevante.	*Probando que:* Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema. Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad. El esquema de clasificación debe incluir criterios para administrar el intercambio de información entre organizaciones, teniendo en cuenta tanto la seguridad y el cumplimiento como la legislación relevante.	Revisión de manuales de procedimientos y funciones Entrevista al jefe de TI.

Cuadro 3.3

Programa de Auditoria PO 4.6

DOMINIO: PLANEACION Y ORGANIZACIÓN	
PO4 Definición de los proceso, organización y las relaciones de TI	
Para conocer si las responsabilidades de seguridad están definidas, entendidas y asignadas apropiadamente.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
PO4.6 Establecimiento de Roles y Responsabilidades El vicerrectorado deberá asignar formalmente la responsabilidad de la seguridad lógica y física de los activos de información de la organización a un jefe de seguridad de la información, quien reportará al mismo. Como mínimo, la responsabilidad del vicerrectorado deberá establecerse a todos los niveles de la organización para manejar los problemas generales de seguridad en la organización. En caso necesario, deberán asignarse responsabilidades gerenciales de seguridad adicionales a niveles específicos con el fin de resolver los problemas de seguridad relacionados con ellos.	□ No existirán procedimientos definidos para el manejo de acciones en caso de problemas de seguridad. □ Falta de planes de contingencia específicos para el manejo de incidentes de seguridad

Cuadro 3.4

Matriz de pruebas PO 4.6

DOMINIO: PLANEACION Y ORGANIZACIÓN		
PO4 Definición de los proceso, organización y las relaciones de TI		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO4.6 Establecimiento de Roles y Responsabilidades El vicerrectorado deberá asignar formalmente la responsabilidad de la seguridad lógica y física de los activos de información de la organización a un jefe de seguridad de la información, quien reportará al mismo. Como mínimo, la responsabilidad del vicerrectorado deberá establecerse a todos los niveles de la organización para manejar los problemas generales de seguridad en la organización.	*Evaluación de controles:* Existen políticas que determinen los roles y responsabilidades para todo el personal dentro de la organización con respecto a sistemas de información, control interno y seguridad. La jefatura ha asignado formalmente la responsabilidad a lo largo de toda la organización para la formulación de políticas y procedimientos de control interno y seguridad (tanto lógica como física) a un oficial de seguridad.	Revisión del documento de descripción de funciones. Entrevista al jefe de área, y colaboradores de TI.

Cuadro 3.4 CONTINUACION

Matriz de pruebas PO 4.6

DOMINIO: PLANEACION Y ORGANIZACIÓN		
PO4 Definición de los proceso, organización y las relaciones de TI		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO4.6 Establecimiento de Roles y Responsabilidades En caso necesario, deberán asignarse responsabilidades gerenciales de seguridad adicionales a niveles especificos con el fin de resolver los problemas de seguridad relacionados con ellos.	*Evaluación de controles:* El oficial de seguridad de la información comprende adecuadamente sus funciones y responsabilidades y si éstas han mostrado consistencia con respecto a la política de seguridad de la información de la organización. Las políticas de seguridad de la organización definen claramente las responsabilidades sobre la seguridad de la información que cada propietario de los activos (por ejemplo, usuarios, administración y administradores de seguridad) debe llevar a cabo. *Probando que:* El personal de seguridad revisa los sistemas operativos y los sistemas de aplicación esenciales.	Revisión del documento de descripción de funciones. Entrevista al jefe de área, y colaboradores de TI.

Cuadro 3.5

Programa de Auditoria PO 4.11

DOMINIO: PLANEACION Y ORGANIZACIÓN	
PO4 Definición de los proceso, organización y las relaciones de TI	
Para conocer si las responsabilidades de seguridad están definidas, entendidas y asignadas apropiadamente.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
PO4.11 Segregación de funciones El vicerrectorado deberá implementar una división de roles y responsabilidades que excluya la posibilidad de que un solo individuo responda por un proceso crítico. La jefatura deberá asegurar también que el personal lleve a cabo únicamente aquellas tareas estipuladas para sus respectivos puestos. En particular, deberá mantenerse una segregación de funciones entre las siguientes funciones: □ uso de sistemas de información; □ entrada de datos; □ operación de cómputo; □ administración de redes; □ administración de sistemas; □ desarrollo y mantenimiento de sistemas □ administración de cambios □ administración de seguridad; y □ auditoria a la seguridad	□ Acceso no autorizado a recursos y datos críticos de TI. □ Confusión en cuanto a los niveles de responsabilidad y de autoridad de los encargados de los procesos de seguridad de TI.

Cuadro 3.6

Matriz de pruebas PO 4.11

DOMINIO: PLANEACION Y ORGANIZACIÓN		
PO4 Definición de los proceso, organización y las relaciones de TI		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO4.11 Segregación de funciones El vicerrectorado deberá implementar una división de roles y responsabilidades que excluya la posibilidad de que un solo individuo responda por un proceso crítico. La jefatura deberá asegurar también que el personal lleve a cabo únicamente aquellas tareas estipuladas para sus respectivos puestos.	*Evaluación de controles:* Existen políticas y procedimientos que describan las prácticas de supervisión para asegurar que las funciones y responsabilidades sean ejercidas apropiadamente y que todo el personal cuente con suficiente autoridad y recursos para llevar a cabo sus funciones y responsabilidades. Existe una segregación de funciones entre los siguientes pares de unidades: - desarrollo y mantenimiento de sistemas - desarrollo y operaciones de sistemas - desarrollo/mantenimiento de sistemas y seguridad de la Información. - operaciones y control de datos - operaciones y usuarios - operaciones y seguridad de la información	Revisión del documento de descripción de funciones. Entrevista al jefe de área, y colaboradores de TI.

Cuadro 3.6 CONTINUACION

Matriz de pruebas PO 4.11

DOMINIO: PLANEACION Y ORGANIZACIÓN		
PO4 Definición de los proceso, organización y las relaciones de TI		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO4.11 Segregación de funciones En particular, deberá mantenerse una segregación de funciones entre las siguientes funciones: □ uso de sistemas de información; □ entrada de datos; □ operación de cómputo; □ administración de redes; □ administración de sistemas; □ desarrollo y mantenimiento de sistemas □ administración de cambios □ administración de seguridad; y □ auditoría a la seguridad	*Probando que:* Las descripciones de los puestos de trabajo tienen claramente delimitada tanto la autoridad como la responsabilidad. La naturaleza y el alcance de la suficiencia de la segregación de funciones deseada y de las limitaciones de funciones dentro de TI. Descripciones de puestos de trabajo apropiadas, para la adecuación y la claridad de las responsabilidades, autoridad y criterios de desempeño.	Revisión del documento de descripción de funciones. Entrevista al jefe de área, y colaboradores de TI.

Cuadro 3.7

Programa de Auditoria PO 6.4

DOMINIO: PLANEACION Y ORGANIZACIÓN	
PO6 Comunicación de las aspiraciones y la dirección de la Gerencia	
Para que las políticas relacionadas con la seguridad de TI sean establecidas y se den a conocer al personal.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
PO6.4 Implantación de políticas de TI La jefatura deberá asegurar que se establezcan procedimientos apropiados para determinar si el personal comprende los procedimientos y políticas implementados, y que éste cumple con dichas políticas y procedimientos. El cumplimiento de las reglas de ética, seguridad y estándares de control interno deberá ser establecido por el vicerrectorado y promoverse a través del ejemplo.	□ Posible uso inadecuado de los recursos y datos de la empresa. □ Fuga de información clave para la empresa. □ Procedimientos no se están realizando según los estándares y no han sido identificados por lo que pueden poner en riesgo la seguridad de los datos.

Cuadro 3.8

Matriz de pruebas PO 6.4

DOMINIO: PLANEACION Y ORGANIZACIÓN		
PO6 Comunicación de las aspiraciones y la dirección de la Gerencia		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO6.4 Implantación de políticas de TI La jefatura deberá asegurar que se establezcan procedimientos apropiados para determinar si el personal comprende los procedimientos y políticas implementados, y que éste cumple con dichas políticas y procedimientos. El cumplimiento de las reglas de ética, seguridad y estándares de control interno deberá ser establecido por la jefatura y promoverse a través del ejemplo.	*Evaluación de controles:* Existen procedimientos apropiados para asegurar que el personal comprende las políticas y procedimientos implementados, y que se cumple con dichas políticas y procedimientos. La administración de la función de servicios de información asegura que la filosofía de calidad, las políticas y objetivos sea comprendida, implementada y mantenida a todos los niveles de la función de servicios de información. *Probando que:* Los esfuerzos de reforzamiento de la administración con respecto a los estándares, directivas, políticas y procedimientos relacionados con su ambiente de control interno están asegurando su cumplimiento a través de	Revisión del documento de descripción de funciones. Entrevista al jefe de área, y colaboradores de TI.

Cuadro 3.9

Programa de Auditoria PO 6.5

DOMINIO: PLANEACION Y ORGANIZACIÓN	
PO6 Comunicación de las aspiraciones y la dirección de la Gerencia	
Para que las políticas relacionadas con la seguridad de TI sean establecidas y se den a conocer al personal.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
PO6.5 Comunicación de los objetivos y la dirección de TI Un programa de concientización sobre seguridad de TI debe comunicar las políticas de TI a cada usuario de TI y asegurar el completo entendimiento de la importancia de la seguridad de TI. Debe transmitir el mensaje en cuanto a que la seguridad de TI es para el beneficio de toda la organización, todos los empleados, y así mismo todos son responsables de ella. El programa de concientización en seguridad de TI debe estar apoyado y representar el punto de vista de la jefatura.	□ Desconocimiento de los usuarios de los procedimientos de seguridad en el manejo de información. □ Fuga de información clave para la empresa. □ Los procedimientos de seguridad de la información no están acorde con los objetivos de la empresa.

Cuadro 3.10

Matriz de pruebas PO 6.5

DOMINIO: PLANEACION Y ORGANIZACIÓN		
PO6 Comunicación de las aspiraciones y la dirección de la Gerencia		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO6.5 Comunicación de los objetivos y la dirección de TI Un programa de concientización sobre seguridad de TI debe comunicar las políticas de TI a cada usuario de TI y asegurar el completo entendimiento de la importancia de la seguridad de TI. Debe transmitir el mensaje en cuanto a que la seguridad de TI es para el beneficio de toda la organización, todos los empleados, y así mismo todos son responsables de ella.	*Evaluación de controles:* Las políticas y procedimientos de la organización crean un marco referencial y un programa de concientización, prestando atención especifica a la tecnología de información, propiciando un ambiente de control positivo y considerando aspectos como: - Integridad - Valores éticos - Código de conducta - Seguridad y control interno - Competencia del personal - Filosofia y estilo operativo de la administración - Responsabilidad, atención y dirección proporcionadas por el consejo directivo o su equivalente	Revisión del documento de descripción de funciones. Entrevista al jefe de área, y colaboradores de TI.

Cuadro 3.10 CONTINUACION

Matriz de pruebas PO 6.5

DOMINIO: PLANEACION Y ORGANIZACIÓN		
PO6 Comunicación de las aspiraciones y la dirección de la Gerencia		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO6.5 Comunicación de los objetivos y la dirección de TI El programa de concientización en seguridad de TI debe estar apoyado y representar el punto de vista de la jefatura.	*Probando que:* Los empleados han recibido el código de conducta y lo comprenden. Miembros seleccionados de la administración están involucrados y comprenden el contenido de las actividades de seguridad y control interno (por ejemplo, reportes de excepción, reconciliaciones, comparaciones, etc.) bajo su responsabilidad. Las funciones individuales, las responsabilidades y líneas de autoridad se comunican claramente y se comprenden en todos los niveles de la organización.	Revisión del documento de descripción de funciones. Entrevista al jefe de área, y colaboradores de TI.

Cuadro 3.11

Programa de Auditoria PO 7.4

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
PO 7 Administrar los Recursos Humanos de TI	
Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y sean conscientes de los riesgos y responsabilidades involucrados.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
PO7.4 Entrenamiento del Personal de TI Todo el personal deberá estar capacitado y entrenado en los principios de seguridad de sistemas, incluyendo actualizaciones periódicas con especial atención en concientización sobre seguridad y manejo de incidentes. El vicerrectorado deberá proporcionar un programa de educación y entrenamiento que incluya: conducta ética de la función de TI, prácticas de seguridad para proteger de una manera segura contra daños que afecten la disponibilidad, la confidencialidad la integridad y el desempeño de las tareas.	□ Desconocimiento de los riesgos de seguridad de TI por parte del personal. □ El personal no aplica los principios y las políticas de seguridad.

Cuadro 3.12

Matriz de pruebas PO 7.4

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
PO 7 Administrar los Recursos Humanos de TI		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO7.4 Entrenamiento del Personal de TI Todo el personal deberá estar capacitado y entrenado en los principios de seguridad de sistemas, incluyendo actualizaciones periódicas con especial atención en concientización sobre seguridad y manejo de incidentes. El vicerrectorado deberá proporcionar un programa de educación y entrenamiento que incluya: conducta ética de la función de TI, prácticas de seguridad para proteger de una manera segura contra daños que afecten la disponibilidad, la confidencialidad la integridad y el desempeño de las tareas.	*Evaluación de objetivos:* El entrenamiento de los empleados incluye un conocimiento y conciencia sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus. El refuerzo a las políticas relacionadas con cargos sensitivos, incluyen: □ se les pide a los empleados en puestos sensitivos que permanezcan alejados de la organización durante un periodo adecuado de tiempo cada año calendario (período de vacaciones; durante éste tiempo su user ID es suspendido; y la persona que reemplaza a el empleado es instruido en el sentido que debe notificar a la administración si nota cualquier anormalidad relacionada con la seguridad). □ la rotación de personal involucrado en actividades sensitivas, sin previa notificación, se realiza de	Revisión de manuales de manejo y uso de los recursos de TI para los empleados. Entrevista al Gerente y/o jefe de TI.

Cuadro 3.12 (continuación)

Matriz de pruebas PO 7.4

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
PO 7 Administrar los Recursos Humanos de TI		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO7.4 Entrenamiento del Personal de TI	*Probando que:* Las responsabilidades de los empleados con respecto a la confidencialidad, integridad, disponibilidad, confiabilidad y seguridad de todos los recursos de TI es comunicada continuamente. Existen programas de entrenamiento vigentes para concientizar a los nuevos y antiguos empleados en seguridad.	

Cuadro 3.13

Programa de Auditoria PO 9.3

DOMINIO: PLANEACION Y ORGANIZACIÓN	
PO9 Evaluar y Administrar los riesgos de TI	
Identificar que puede ir mal con la seguridad de TI y su impacto en los objetivos del negocio, considerar como asegurar datos y transacciones que son críticos para el negocio, preparar un plan de acción para manejo de riesgos y concienciar al personal sobre los riesgos de seguridad.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
PO9.3 Identificación de Eventos La evaluación de riesgos deberá enfocarse al examen de los elementos esenciales de riesgo y las relaciones causa/efecto entre ellos. Los elementos esenciales de riesgo incluyen activos tangibles e intangibles, amenazas, valor de los activos, vulnerabilidades, protecciones, consecuencias y probabilidad de amenaza. El proceso de identificación de riesgos debe incluir una clasificación cualitativa y, donde sea apropiado, clasificación cuantitativa de riesgos y debe obtener insumos de las tormentas de ideas de la jefatura y vicerrectorado, de planeación estratégica, auditorías anteriores y otros análisis. El análisis de riesgos debe considerar el negocio, regulaciones, aspectos legales, tecnología, comercio entre	□ Una inadecuada evaluación de riesgos de la seguridad en la red informática no permitirá medir el impacto de un ataque a la seguridad. □ No se identifica de manera clara las Áreas vulnerables y Áreas Críticas en cuando a seguridad de la red informática. □ Riesgos no identificados no tendrán un plan de contingencia para su inmediata recuperación. □ No se tendría conocimiento de los perjuicios económicos ocasionados por los problemas de seguridad en la red informática.

Cuadro 3.14

Matriz de pruebas PO 9.3

DOMINIO: PLANEACION Y ORGANIZACIÓN		
PO9 Evaluar y Administrar los riesgos de TI		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO9.3 Identificación de Eventos La evaluación de riesgos deberá enfocarse al examen de los elementos esenciales de riesgo y las relaciones causa/efecto entre ellos. Los elementos esenciales de riesgo incluyen activos tangibles e intangibles, vulnerabilidades, valor de los activos, amenazas, protecciones, consecuencias y probabilidad de amenaza. El proceso de identificación de riesgos debe incluir una clasificación cualitativa y, donde sea apropiado, clasificación cuantitativa de riesgos y debe obtener insumos de las tormentas de ideas de la jefatura, de planeación estratégica, auditorías anteriores y otros análisis. El análisis de riesgos debe considerar el negocio, regulaciones, aspectos legales, tecnología, comercio entre socios y riesgos del recurso humano.	*Evaluación de controles:* Los objetivos de toda la organización están incluidos en el proceso de identificación de riesgos. Se incluyen técnicas de probabilidad, frecuencia y análisis de amenazas en la identificación de riesgos. Existe un enfoque cuantitativo y/o cualitativo (o combinado) formal para la identificación y medición de riesgos, amenazas y exposiciones. *Probando que:* La administración comprende los factores relacionados con los riesgos y la probabilidad de amenazas Los reportes emitidos a la Presidencia para su revisión y acuerdo con los riesgos identificados y utilización en el monitoreo de actividades de reducción de	Recopilación de planes de contingencia. Entrevista con el jefe de TI.

Cuadro 3.15

Programa de Auditoria PO 9.5

DOMINIO: PLANEACION Y ORGANIZACIÓN	
PO9 Evaluar y Administrar los riesgos de TI	
Identificar que puede ir mal con la seguridad de TI y su impacto en los objetivos del negocio, considerar como asegurar datos y transacciones que son criticos para el negocio, preparar un plan de acción para manejo de riesgos y concienciar al personal sobre los riesgos de seguridad.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
PO9.5 Respuesta a los Riesgos El enfoque de evaluación de riesgos deberá proporcionar la definición de un plan de acción contra riesgos para asegurar que el costo–efectividad de los controles y las medidas de seguridad mitiguen los riesgos en forma continua. El plan de acción contra los riesgos debe identificar la estrategia de riesgos en términos de evitar, mitigar o aceptar el riesgo.	□ Demora o pérdida de los servicios que brinda la red. □ Pérdidas económicas ocasionadas por falta o deficiencia del servicio de red.

Cuadro 3.16

Matriz de pruebas PO 9.5

DOMINIO: PLANEACION Y ORGANIZACIÓN		
PO9 Evaluar y Administrar los riesgos de TI		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
PO9.5 Respuesta a los Riesgos El enfoque de evaluación de riesgos deberá proporcionar la definición de un plan de acción contra riesgos para asegurar que el costo– efectividad de los controles y las medidas de seguridad mitiguen los riesgos en forma continua. El plan de acción contra los riesgos debe identificar la estrategia de riesgos en términos de evitar, mitigar o aceptar el riesgo.	*Evaluación de controles:* Existen procedimientos para el monitoreo y el mejoramiento continuos de la evaluación de riesgos y procesos para la creación de controles que mitiguen los riesgos. El plan de acción contra riesgos es utilizado en la implementación de medidas apropiadas para mitigar los riesgos, amenazas y exposiciones. *Probando que:* El plan de acción contra riesgos es actual e incluye controles económicos y medidas de seguridad para mitigar la exposición al riesgo. Se han priorizado los riesgos desde el más alto hasta el más bajo y existe una respuesta apropiada para cada riesgo.	Revisión de los planes de contingencia.

3.2 Procesos del Dominio Adquisición e Implementación

Cuadro 3.17

Programa de Auditoria AI 3.2

DOMINIO: ADQUISICION E IMPLEMENTACION	
AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica	
Se refiere a la seguridad apropiada para la infraestructura tecnológica (hardware y software) que tiene que ver con la actualización, mantenimiento y adquisición.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
AI3.2 Protección y Disponibilidad del recurso de infraestructura. La jefatura de la función de servicios de información deberá asegurar que la instalación del software del sistema no arriesgue la seguridad de los datos y programas ya almacenados en el mismo. Deberá prestarse gran atención a la instalación y mantenimiento de los parámetros del software del sistema.	□ Mayor exposición de las vulnerabilidades del sistema al no contar con parches actualizados. □ Fallas en la integridad de los datos. □ Falla en el funcionamiento de las aplicaciones de red.

Cuadro 3.18

Matriz de pruebas AI 3.2

DOMINIO: ADQUISICION E IMPLEMENTACION		
AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
AI3.2 Protección y Disponibilidad del recurso de infraestructura. La jefatura de la función de servicios de información deberá asegurar que la instalación del software del sistema no arriesgue la seguridad de los datos y programas ya almacenados en el mismo. Deberá prestarse gran atención a la instalación y mantenimiento de los parámetros del software	*Evaluación de controles:* Existen politicas y procedimientos que aseguran que: - la posibilidad de acceso al software del sistema y con ella, la posibilidad de interrumpir los sistemas de información operativa está limitada - la preparación, instalación y mantenimiento del software del sistema no amenaza la seguridad de los datos y programas almacenados en el sistema. - se seleccionan parámetros del software del sistema para asegurar la integridad de los datos y programas almacenados en el sistema. *Probando que:* Existen las declaraciones de aseguramiento de la integridad del software del sistema entregados por los proveedores para todo el software del sistema (incluyendo todas las modificaciones) y considera las exposiciones resultantes en el software del sistema. Los parámetros del software del sistema aseguran que el personal apropiado de TI seleccionó los correctos con el fin de asegurar la	Aplicación de listado de chequeo al jefe de TI.

Cuadro 3.19

Programa de Auditoria AI 3.3

DOMINIO: ADQUISICION E IMPLEMENTACION	
AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica	
Se refiere a la seguridad apropiada para la infraestructura tecnológica (hardware y software) que tiene que ver con la actualización, mantenimiento y adquisición.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
AI3.3 Mantenimiento de la Infraestructura La jefatura de la función de servicios de información deberá agendar o programar el mantenimiento rutinario y periódico del hardware con el fin de reducir la frecuencia y el impacto de fallas de rendimiento.	□ Daño permanente de los equipos. □ Fallo en el servicio en caso de daños de equipos de interconexión. □ Incremento de gastos por reparación de equipos. □ Usuarios insatisfechos.

Cuadro 3.20

Matriz de pruebas AI 3.3

DOMINIO: ADQUISICION E IMPLEMENTACION		
AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
AI3.3 Mantenimiento de la Infraestructura La jefatura de la función de servicios de información deberá agendar o programar el mantenimiento rutinario y periódico del hardware con el fin de reducir la frecuencia y el impacto de fallas de rendimiento.	*Evaluación de controles:* Existen políticas y procedimientos para el mantenimiento preventivo de hardware para reducir la frecuencia y el impacto de las fallas de desempeño Se cumple con los pasos y la frecuencia de mantenimiento preventivo prescritos por el proveedor para cada dispositivo de hardware operado por la función de servicios de información y los usuarios afectados se adhieren a ellos. *Probando que:* El calendario de mantenimiento preventivo asegura que el mantenimiento de hardware programado no tendrá ningún impacto negativo sobre aplicaciones críticas o sensitivas. El mantenimiento programado asegura que no ha sido planeado para periodos pico de carga de trabajo y que la función de servicios de información y las operaciones de los grupos de usuarios afectados son suficientemente flexibles para adaptar el mantenimiento preventivo rutinario planeado. Los programas operativos de servicios de información aseguran que existen las preparaciones adecuadas para manejar anticipadamente los tiempos muertos de	Entrevista al jefe de TI. Revisión del Contrato de Mantenimiento de Hardware.

3.3 Proceso del Dominio de Entrega y Soporte

Cuadro 3.21

Programa de Auditoria DS 2.3

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS2 Administración de Servicios Prestados por Terceros	
Se refiere a la definición en cuanto a los aspectos de seguridad, confidencialidad y continuidad de los servicios prestados por terceros.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS2.3 Administración de Riesgos del Proveedor Con respecto a las relaciones con los proveedores de servicios como terceras partes, la jefatura deberá asegurar que los acuerdos de seguridad (por ejemplo, los acuerdos de confidencialidad) sean identificados, declarados explícitamente y acordados, que éstos concuerden con los estándares de negocios universales y estén en linea con los requerimientos legales y regulatorios, incluyendo obligaciones.	□ Acceso no autorizado a información confidencial. □ Pérdida de información crítica. □ Responsabilidad legal no asumida por parte de terceros en caso de presentarse problemas de seguridad.

Cuadro 3.22

Matriz de pruebas DS 2.3

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS2 Administración de Servicios prestados por Terceros		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS2.3 Administración de Riesgos del Proveedor Con respecto a las relaciones con los proveedores de servicios como terceras partes, la jefatura deberá asegurar que los acuerdos de seguridad (por ejemplo, los acuerdos de confidencialidad) sean identificados, declarados explícitamente y acordados, que éstos concuerden con los estándares de negocios universales y estén en linea con los requerimientos legales y regulatorios, incluyendo obligaciones.	*Evaluación de controles:* El contenido de los contratos incluye por lo menos: - requerimientos de seguridad - garantías de confidencialidad *Probando que:* El contenido de los contratos incluye por lo menos: - requerimientos de seguridad - garantías de confidencialidad La lista de seguridad de acceso incluye únicamente un número mínimo de proveedores requeridos, y que dicho acceso es el mínimo necesario.	Revisión de contratos con proveedores de servicios. Entrevista al jefe de TI.

Cuadro 3.23

Programa de Auditoria DS 4.2

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS4 Garantizar la continuidad del servicio	
Se refiere a la capacidad de la empresa de seguir brindando el servicio contando con un plan de contingencias para la recuperación de fallas después de incidentes en un tiempo mínimo y disponer de respaldos confiables.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS4.2 Planes de Continuidad de TI La jefatura de TI deberá asegurar que se desarrolle un plan escrito conteniendo lo siguiente: - Guías sobre la utilización del Plan de Continuidad; - Procedimientos de emergencia para asegurar la integridad de todo el personal afectado; - Procedimientos de respuesta definidos para regresar al negocio al estado en que se encontraba antes del incidente o desastre; - Procedimientos para salvaguardar y reconstruir las instalaciones; - Procedimientos de coordinación con las autoridades públicas; - Procedimientos de comunicación con los socios y demás interesados: empleados, clientes clave, proveedores críticos, accionistas y gerencia; y - Información crítica sobre grupos de continuidad, personal afectado, clientes, proveedores, autoridades públicas y medios de comunicación.	□ Pérdidas económicas para empresa. □ Demora en la recuperación o pérdida de los servicios de red. □ Pérdida o daño de información crítica. □ Plan de contingencia no actualizado e incompleto.

Cuadro 3.24

Matriz de pruebas DS 4.2

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS4 Garantizar la continuidad del servicio		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS4.2 Contenido del Plan de Continuidad de TI La jefatura de TI deberá asegurar que se desarrolle un plan escrito conteniendo: - Guías sobre la utilización del Plan de Continuidad; - Procedimientos de emergencia para asegurar la integridad de todo el personal afectado; - Procedimientos de respuesta definidos para regresar al negocio al estado en que se encontraba antes del incidente o desastre; - Procedimientos para salvaguardar y reconstruir las instalaciones; - Procedimientos de coordinación con las autoridades públicas; - Procedimientos de comunicación con los socios y demás interesados: empleados, clientes clave, proveedores críticos, accionistas y gerencia; y - Información crítica sobre grupos de continuidad, personal afectado, clientes, proveedores,	*Evaluación de controles:* La inclusión de los siguientes puntos como contenido mínimo en cada plan de continuidad: - Procedimientos de emergencia para garantizar la seguridad de todos los miembros del personal afectados. *Probando que:* Se han dado el entrenamiento y la concientización de los usuarios y del personal de la función de servicios de información en cuanto a funciones, tareas y responsabilidades específicas dentro del plan.	Revisión de los Planes de Contingencia existentes.

Cuadro 3.25

Programa de Auditoria DS 4.3

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS4 Garantizar la continuidad del servicio	
Se refiere a la capacidad de la empresa de seguir brindando el servicio contando con un plan de contingencias para la recuperación de fallas después de incidentes en un tiempo mínimo y disponer de respaldos confiables.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS4.3 Recursos críticos de tecnología de información El plan de continuidad deberá identificar los programas de aplicación, servicios de terceros, sistemas operativos, personal, insumos, archivos de datos que resultan críticos así como los tiempos necesarios para la recuperación después de que se presenta un desastre. Los datos y las operaciones críticas deben ser identificadas, documentadas, priorizadas y aprobadas por los dueños de los procesos del negocio en cooperación con la jefatura de TI.	□ No se asegura el funcionamiento continuo de aplicaciones de red, servidores y servicio de terceros. □ No estimación de los tiempos de recuperación. □ Pérdida o daño de información crítica.

Cuadro 3.26

Matriz de pruebas DS 4.3

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS4 Garantizar la continuidad del servicio		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS4.3 Recursos criticos de tecnología de información El plan de continuidad deberá identificar los programas de aplicación, servicios de terceros, sistemas operativos, personal, insumos, archivos de datos que resultan críticos así como los tiempos necesarios para la recuperación después de que se presenta un desastre. Los datos y las operaciones críticas deben ser identificadas, documentadas, priorizadas y aprobadas por los dueños de los procesos del negocio en cooperación con la jefatura de TI.	*Evaluación de controles:* - Una lista de los recursos de sistemas que requieren alternativas (hardware, periféricos, software). - Una lista de las aplicaciones priorizadas de mayor a menor, de los tiempos de recuperación requeridos y de las normas de desempeño esperadas. - La identificación de equipo especifico y necesidades de suministros tales como impresoras de alta velocidad, firmas, formatos, equipo de comunicación, teléfonos, etc., así como de una fuente y otras fuentes alternativas definidas. *Probando que:* La jefatura aprueba la información y operaciones críticas.	Aplicación de listado de chequeo al jefe de TI.

Cuadro 3.27

Programa de Auditoria DS 4.5

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS4 Garantizar la continuidad del servicio	
Se refiere a la capacidad de la empresa de seguir brindando el servicio contando con un plan de contingencias para la recuperación de fallas después de incidentes en un tiempo mínimo y disponer de respaldos confiables.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS4.5 Pruebas del Plan de continuidad de TI Para contar con un Plan efectivo de Continuidad, la gerencia necesita evaluar su adecuación de manera regular o cuando se presenten cambios mayores en el negocio o en la infraestructura de TI; esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas e implementar un plan de acción de acuerdo con los resultados.	□ Plan de contingencia no efectivo, no eficiente.

Cuadro 3.28

Matriz de pruebas DS 4.5

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS4 Garantizar la continuidad del servicio		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS4.5 Pruebas del Plan de continuidad de TI Para contar con un Plan efectivo de Continuidad, la gerencia necesita evaluar su adecuación de manera regular o cuando se presenten cambios mayores en el negocio o en la infraestructura de TI; esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas e implementar un plan de acción de acuerdo con los resultados.	*Evaluación de controles*: La programación de pruebas, los resultados de la última prueba y las acciones correctivas llevadas a cabo tomando como base la(s) prueba(s) anterior(es). *Probando que:* El plan ha sido probado recientemente y que éste trabajó de acuerdo con lo esperado, o que cualquier deficiencia encontrada trajo como resultado la aplicación de correcciones al plan.	Solicitar informe de resultado de las pruebas del plan de contingencia. Entrevista al jefe de TI..

Cuadro 3.29

Programa de Auditoria DS 4.8

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS4 Garantizar la continuidad del servicio	
Se refiere a la capacidad de la empresa de seguir brindando el servicio contando con un plan de contingencias para la recuperación de fallas después de incidentes en un tiempo mínimo y disponer de respaldos confiables.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS4.8 Recuperación y Reanudación de los servicios de TI La metodología de continuidad deberá asegurar que los departamentos usuarios establezcan procedimientos alternativos de procesamiento, que puedan ser utilizados hasta que la función de servicios de información sea capaz de restaurar completamente sus servicios después de un evento o un desastre.	□ Procedimiento alternativo no funciona adecuadamente y no permita seguir operando. □ Pérdida de información crítica. □ Interrupción en las labores de los usuarios por falta del servicio.

Cuadro 3.30

Matriz de pruebas DS 4.8

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS4 Garantizar la continuidad del servicio		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS4.8 Recuperación y Reanudación de los servicios de TI La metodología de continuidad deberá asegurar que los departamentos usuarios establezcan procedimientos alternativos de procesamiento, que puedan ser utilizados hasta que la función de servicios de información sea capaz de restaurar completamente sus servicios después de un evento o un desastre.	*Evaluación de controles:* Las alternativas de reanudación del negocio para todos los usuarios estableciendo sitios de trabajo alternativo, una vez que los recursos de sistemas de información estén disponibles (por ejemplo, el sistema ha sido recuperado en el sitio alterno pero el edificio de los usuarios sufrió un incendio y no está disponible). Los planes de contingencia para usuarios son desarrollados tomando como base la no disponibilidad de los recursos físicos para llevar a cabo procesamientos críticos - manuales y computarizados. *Probando que:* Los procedimientos manuales alternativos son documentados y probados como parte de la prueba global.	Recopilación y revisión de Documentos con procedimientos de respaldo.

Cuadro 3.31

Programa de Auditoria DS 4.9

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS4 Garantizar la continuidad del servicio	
Se refiere a la capacidad de la empresa de seguir brindando el servicio contando con un plan de contingencias para la recuperación de fallas después de incidentes en un tiempo mínimo y disponer de respaldos confiables.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS4.9 Almacenamiento de respaldo fuera de las instalaciones El almacenamiento externo de copias de respaldo, documentación y otros recursos tecnológicos de información, catalogados como críticos, debe ser establecido para soportar el plan de recuperación y continuidad del negocio. Los propietarios de los procesos del negocio y el personal de la función de TI deben involucrarse en determinar que recursos de respaldo deben ser almacenados en el sitio alterno. La instalación de almacenamiento externo debe contar con medidas ambientales para los medios y otros recursos almacenados; y debe tener un nivel de seguridad suficiente, que permita proteger los recursos de respaldo contra accesos no autorizados, robo o daño. El vicerrectorado debe asegurar que los acuerdos/contratos del sitio alterno son periódicamente analizados, al menos una vez al año, para garantizar que ofrezca seguridad y protección	□ No existen respaldos guardados en sitios externos. □ Daño en los dispositivos de respaldo por el medioambiente inadecuado para almacenamiento. □ Fracaso del Plan de Contingencia.

Cuadro 3.32

Matriz de pruebas DS 4.9

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS4 Garantizar la continuidad del servicio		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS4.9 Almacenamiento de respaldo fuera de las instalaciones El almacenamiento externo de copias de respaldo, documentación y otros recursos tecnológicos de información, catalogados como críticos, debe ser establecido para soportar el plan de recuperación y continuidad del negocio. Los propietarios de los procesos del negocio y el personal de la función de TI deben involucrarse en determinar que recursos de respaldo deben ser almacenados en el sitio alterno.	*Evaluación de controles:* El detalle de los proveedores de servicios contratados, de los servicios y de las expectativas de respuesta. La información logística de la localización de recursos claves, incluyendo el centro de cómputo de respaldo para la recuperación de sistemas operativos, aplicaciones, archivos de datos, manuales de operación y documentación de programas / sistema / usuarios. Los sistemas de imágenes, los sistemas de fax, los documentos en papel asi como los microfilm y los medios de almacenamiento son parte del plan de continuidad.	Entrevista al jefe de TI.

Cuadro 3.32 CONTINUACION

Matriz de pruebas DS 4.9

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS4 Garantizar la continuidad del servicio		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS4.9 Almacenamiento de respaldo fuera de las instalaciones La instalación de almacenamiento externo debe contar con medidas ambientales para los medios y otros recursos almacenados; y debe tener un nivel de seguridad suficiente, que permita proteger los recursos de respaldo contra accesos no autorizados, robo o daño. La jefatura de TI debe asegurar que los acuerdos/contratos del sitio alterno son periódicamente analizados, al menos una vez al año, para garantizar que ofrezca seguridad y protección ambiental.	*Probando que:* Las relaciones y tiempos del proveedor contratado son consistentes con las expectativas y necesidades del usuario. El contenido del sitio de respaldo está actualizado y es suficiente con respecto a los procedimientos normales de rotación en el sitio alterno (off-site).	Entrevista al jefe de TI.

Cuadro 3.33

Programa de Auditoria DS 5.1

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS5 Garantizar la seguridad de Sistemas	
Contempla el control de acceso a sistemas para los diferentes usuarios, detectar, reportar y solucionar incidentes de violación de seguridad, protección de respaldos, etc.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS5.1 Administración de la seguridad de TI La seguridad en TI deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye: □ Trasladar información sobre evaluación de riesgos a los planes de seguridad de TI; □ Implementar el plan de seguridad de TI; □ Actualizar el plan de seguridad de TI para reflejar cambios en la configuración de TI; □ Evaluar el impacto de las solicitudes de cambio en la seguridad de TI; □ Monitorear la implementación del plan de seguridad de TI; y □ Alinear los procedimientos de seguridad de TI a otras políticas y procedimientos	□ La no evaluación de riesgos sobre TI ni su impacto en el cumplimiento de los objetivos del negocio. □ La no definición de un plan de seguridad específico de TI.

Cuadro 3.34

Matriz de pruebas DS 5.1

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS5 Garantizar la seguridad de Sistemas		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS5.1 Administración de la seguridad de TI La seguridad en TI deberá ser administrada de tal forma que las medidas de seguridad se encuentren en línea con los requerimientos de negocio. Esto incluye: □ Trasladar información sobre evaluación de riesgos a los planes de seguridad de TI; □ Implementar el plan de seguridad de TI; □ Actualizar el plan de seguridad de TI para reflejar cambios en la configuración de TI; □ Evaluar el impacto de las solicitudes de cambio en la seguridad de TI; □ Monitorear la implementación del plan de seguridad de TI; y □ Alinear los procedimientos de seguridad de TI a otras políticas y procedimientos	*Evaluación de controles:* Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario, como soporte *Probando que:* Los parámetros de seguridad del sistema tienen como base estándares locales/del proveedor	Solicitar documento de políticas de seguridad. Entrevista al jefe de TI. Revisión del Plan de Contingencia.

Cuadro 3.35

Programa de Auditoria DS 5.3

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS5 Garantizar la seguridad de Sistemas	
Contempla el control de acceso a sistemas para los diferentes usuarios, detectar, reportar y solucionar incidentes de violación de seguridad, protección de respaldos, etc.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS5.3 Administración de Identidad El acceso lógico y el uso de los recursos de TI deberán restringirse a través de la implementación de mecanismos adecuados de identificación, autenticación y autorización relacionando los usuarios y los recursos con las reglas de acceso. Dicho mecanismo deberá evitar que personal no autorizado, conexiones telefónicas por marcado y otros puertos de entrada al sistema (redes) tengan acceso a los recursos de cómputo. Asimismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso (por ejemplo, cambios periódicos de contraseñas o passwords).	□ Falta o deficiencia en los mecanismos de seguridad para el control de acceso a los recursos de TI. □ Falta de evaluación y corrección de los mecanismos de control.

Cuadro 3.36

Matriz de pruebas DS 5.3

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS5 Garantizar la seguridad de Sistemas		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS5.3 Administración de Identidad El acceso lógico y el uso de los recursos de TI deberán restringirse a través de la implementación de mecanismos adecuados de identificación, autenticación y autorización relacionando los usuarios y los recursos con las reglas de acceso. Dicho mecanismo deberá evitar que personal no autorizado, conexiones telefónicas por marcado y otros puertos de entrada al sistema (redes) tengan acceso a los recursos de cómputo. Asimismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso.	*Evaluación de controles:* Se cuenta con perfiles de seguridad de usuario que representen "los menos accesos requeridos" y que muestren revisiones regulares a los perfiles por parte de la administración con fines de re acreditación. Los mecanismos de autenticidad en uso proveen las siguientes facilidades: • uso individual de datos de autenticación • autentificación múltiple • autenticación basada en políticas • Autenticación por demanda La política de contraseñas incluye: • Forzar el cambio inicial de password la primera vez de uso • longitud adecuada mínima de las contraseñas • la frecuencia obligada mínima de cambio de password • verificación del password en la lista de valores no permitidos y protección adecuada para los passwords	Entrevista al jefe de TI. Correr herramienta que ayude a detectar problemas con claves y vulnerabilidades de seguridad en los servidores de aplicación.

Cuadro 3.36 (continuación)

Matriz de pruebas DS 5.3

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS5 Garantizar la seguridad de Sistemas		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS5.3 Administración de Identidad El acceso lógico y el uso de los recursos de TI deberán restringirse a través de la implementación de mecanismos adecuados de identificación, autenticación y autorización relacionando los usuarios y los recursos con las reglas de acceso. Dicho mecanismo deberá evitar que personal no autorizado, conexiones telefónicas por marcado y otros puertos de entrada al sistema (redes) tengan acceso a los recursos de cómputo. Asimismo deberán establecerse procedimientos para conservar la efectividad de los mecanismos de autenticación y acceso (por ejemplo, cambios periódicos de contraseñas o passwords)	Los procedimientos de marcación telefónica incluyen autenticación basada en token o dial-back, cambios frecuentes del número telefónico, firewalls de hardware y software para restringir el acceso a los activos y cambios frecuentes de las claves de acceso y desactivación de las claves de acceso de los empleados temporales. *Probando que:* TI cumple con los estándares de seguridad relacionados con: • autenticación y acceso • administración de perfiles de usuario y clasificación de la seguridad de datos Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema.	

Cuadro 3.37

Programa de Auditoria DS 5.4

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS5 Garantizar la seguridad de Sistemas	
Contempla el control de acceso a sistemas para los diferentes usuarios, detectar, reportar y solucionar incidentes de violación de seguridad, protección de respaldos, etc.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS5.4 Administración de cuentas de usuario La jefatura deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre de cuentas de usuario. Deberá incluirse un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso. La seguridad de acceso a terceros debe definirse contractualmente teniendo en cuenta requerimientos de administración y no revelación. Los acuerdos de outsourcing deben considerar los riesgos, los controles sobre seguridad y los procedimientos para los sistemas de información y las redes en el contrato que se establece entre las partes.	□ Cuentas de usuario habilitadas de personal que ya no trabaja en la empresa. □ Ataques maliciosos a la información.

Cuadro 3.38

Matriz de pruebas DS 5.4

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS5 Garantizar la seguridad de Sistemas		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS5.4 Administración de cuentas de usuario La jefatura deberá establecer procedimientos para asegurar acciones oportunas relacionadas con la solicitud, establecimiento, emisión, suspensión y cierre de cuentas de usuario. Deberá incluirse un procedimiento de aprobación formal que indique el propietario de los datos o del sistema que otorga los privilegios de acceso.	*Evaluación de controles:* El número de sesiones concurrentes correspondientes al mismo usuario están limitadas. La política de contraseñas incluye: Forzar el cambio inicial de claves la primera vez de uso - longitud adecuada mínima del password sistemas –la frecuencia obligada mínima de cambio de la misma. Verificación de claves en la lista de valores no permitidos (Ej., verificación de diccionario). Protección adecuada para las claves de emergencia. Se cuenta con reportes de fallas a la seguridad y procedimientos formales de solución de problemas. Estos reportes deberán incluir: • intentos no autorizados de acceso al sistema • intentos no autorizados de acceso a los recursos del sistema • privilegios de acceso a recursos por ID de usuario • modificaciones autorizadas a las definiciones y reglas de seguridad • accesos autorizados a los recursos	Solicitar documento de políticas de seguridad. Entrevista al jefe de TI.

Cuadro 3.38 CONTINUACION

Matriz de pruebas DS 5.4

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS5 Garantizar la seguridad de Sistemas		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS5.4 Administración de cuentas de usuario La seguridad de acceso a terceros debe definirse contractualmente teniendo en cuenta requerimientos de administración y no revelación. Los acuerdos de outsourcing deben considerar los riesgos, los controles sobre seguridad y los procedimientos para los sistemas de información y las redes en el contrato que se establece entre las partes.	*Probando que:* Cumple con los estándares de seguridad relacionados con: - Autenticación de usuarios. - Administración de perfiles de usuario y clasificación de la seguridad de datos. - Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema. - Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad.	Solicitar documento de políticas de seguridad. Entrevista al jefe de TI.

Cuadro 3.39

Programa de Auditoria DS 5.5

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS5 Garantizar la seguridad de Sistemas	
Contempla el control de acceso a sistemas para los diferentes usuarios, detectar, reportar y solucionar incidentes de violación de seguridad, protección de respaldos, etc.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS5.5 Pruebas, Vigilancia y Monitoreo de la seguridad La administración de seguridad de TI debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente a todos aquellos que puedan verse afectada, tanto interna como externamente y se debe actuar de una manera oportuna.	□ No se determina responsables directo o indirecto de un incidente de seguridad. □ No puede determinar origen, fecha y hora del incidente de seguridad. □ No se toman acciones de forma inmediata para superar el incidente.

Cuadro 3.40

Matriz de pruebas DS 5.5

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS5 Garantizar la seguridad de Sistemas		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS5.5 Pruebas, Vigilancia y Monitoreo de la seguridad La administración de seguridad de TI debe asegurar que la actividad de seguridad sea registrada y que cualquier indicación sobre una inminente violación de seguridad sea notificada inmediatamente a todos aquellos que puedan verse afectada, tanto interna como externamente y se debe actuar de una manera oportuna	*Evaluación de controles:* Se cuenta con reportes de fallas a la seguridad y procedimientos formales de solución de problemas. Estos reportes deberán incluir: - Intentos no autorizados de acceso al sistema - Intentos no autorizados de acceso a los recursos del sistema. - Intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad. - Privilegios de acceso a recursos por ID de usuario. - Modificaciones autorizadas a las definiciones y reglas de seguridad de TI. - Accesos autorizados a los recursos - Cambio de estatus de la seguridad del sistema. - Accesos a las tablas de parámetros de seguridad del sistema operativo. *Probando que*: TI cumple con los estándares de seguridad relacionados con: reportes y revisión gerencial de las violaciones e incidentes de seguridad. Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta	Revisión de manuales de procedimientos y plan de contingencia. Entrevista al jefe de TI.

Cuadro 3.41

Programa de Auditoria DS 5.6

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS5 Garantizar la seguridad de Sistemas	
Contempla el control de acceso a sistemas para los diferentes usuarios, detectar, reportar y solucionar incidentes de violación de seguridad, protección de respaldos, etc.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS5.6 Definición de Incidente de Seguridad La jefatura deberá implementar la capacidad de manejar incidentes de seguridad computacional, dar atención a dichos incidentes mediante el establecimiento de una plataforma centralizada con suficiente experiencia y equipada con instalaciones de comunicación rápidas y seguras. Deberán establecerse las responsabilidades y los procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna a los incidentes de seguridad.	□ No se notifiquen oportunamente los incidentes de seguridad. □ El plan de contingencia no se aplica satisfactoriamente. □ Falla o pérdida de los servicios de red □ Pérdida o daño de información crítica.

Cuadro 3.42

Matriz de pruebas DS 5.6

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS5 Garantizar la seguridad de Sistemas		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS5.6 Definición de Incidente de Seguridad La jefatura deberá implementar la capacidad de manejar incidentes de seguridad computacional, dar atención a dichos incidentes mediante el establecimiento de una plataforma centralizada con suficiente experiencia y equipada con instalaciones de comunicación rápidas y seguras. Deberán establecerse las responsabilidades y los procedimientos de manejo de incidentes para asegurar una respuesta apropiada, efectiva y oportuna a los incidentes de seguridad.	*Evaluación de controles:* Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario, como soporte. Se utilizan rutas confiables para transmitir información sensitiva. Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador. *Probando que:* Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes.	Revisión del plan de contingencia. Entrevista al jefe de TI.

Cuadro 3.43

Programa de Auditoria DS 5.9

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS5 Garantizar la seguridad de Sistemas	
Contempla el control de acceso a sistemas para los diferentes usuarios, detectar, reportar y solucionar incidentes de violación de seguridad, protección de respaldos, etc.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS5.9 Prevención, detección y corrección de software malicioso Con respecto al software malicioso, tal como los virus computacionales o Caballos de Troya, la jefatura deberá establecer un marco de referencia de adecuadas medidas de control preventivas, detectivas y correctivas y responder y reportar su presencia. Las Gerencias y/o jefaturas de TI y de negocios deben asegurar que se establezcan procedimientos a través de toda la organización para proteger los sistemas de información contra virus computacionales. Los procedimientos deben incorporar protección contra virus, detección, respuesta ante su presencia y reporte.	□ Ataque de virus, spyware, troyanos, etc. □ Colapso en el funcionamiento de los servicios de red. □ Daño de información.

Cuadro 3.44

Matriz de pruebas DS 5.9

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS5 Garantizar la seguridad de Sistemas		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS5.9 Prevención, detección y corrección de software malicioso Con respecto al software malicioso, tal como los virus computacionales o Caballos de Troya, la jefatura deberá establecer un marco de referencia de adecuadas medidas de control preventivas, detectivas y correctivas y responder y reportar su presencia. Las jefaturas de TI y de negocios deben asegurar que se establezcan procedimientos a través de toda la organización para proteger los sistemas de información contra virus computacionales. Los procedimientos deben incorporar protección contra virus, detección,	*Evaluación de controles:* El entrenamiento de los empleados incluye un conocimiento y conciencia sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus. Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador. *Probando que:* Los procedimientos para la protección contra software malicioso incluyen: □ todo el software adquirido por la organización se revisa contra los virus antes de su instalación y uso. □ existe una política por escrito sobre descargue de archivos, aceptación y uso de software,	Revisión de manuales de manejo y uso de los recursos de TI para los empleados. Entrevista al Gerente y/o jefe de TI.

Cuadro 3.44 (continuación)

Matriz de pruebas DS 5.9

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS5 Garantizar la seguridad de Sistemas		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS5.9 Prevención, detección y corrección de software malicioso	□ el software para aplicaciones altamente sensibles está protegido por MAC (Código de Autentificación de Mensajes) o firma digital, y se utilizan mecanismos, fallas de verificación para evitar el uso del software. □ los usuarios tienen instrucciones para la detección y reportes de virus, como el desempeño lento o crecimiento misterioso de archivos. □ existe una política y un procedimiento vigente para la verificación de disquetes obtenidos por fuera del programa de compra normal de la organización.	Revisión de manuales de manejo y uso de los recursos de TI para los empleados. Entrevista al jefe de TI.

Cuadro 3.45

Programa de Auditoria DS 5.10

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS5 Garantizar la seguridad de Sistemas	
Contempla el control de acceso a sistemas para los diferentes usuarios, detectar, reportar y solucionar incidentes de violación de seguridad, protección de respaldos, etc.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS5.10 Seguridad de la Red La organización deberá contar con *Firewall* adecuados para proteger contra negación de servicios y cualquier acceso no autorizado a los recursos internos, si existe conexión con Internet u otras redes públicas, se deberá controlar en ambos sentidos cualquier aplicación y el flujo de administración de infraestructura y se deberá proteger contra ataques de negación del servicio.	□ Intrusos en la red de la organización. □ Ataques a los recursos de la red. □ Posible acceso externo directo a ciertos servicios internos de la red. □ Ataques de software malicioso, virus, etc. □ Gran cantidad de ataques basados en SMTP, se puede pasar por alto el tráfico entrante y filtrado de manera acorde.

Cuadro 3.46

Matriz de pruebas DS 5.10

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS5 Garantizar la seguridad de Sistemas		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS5.10 Seguridad de la Red La organización deberá contar con *Firewall* adecuados para proteger contra negación de servicios y cualquier acceso no autorizado a los recursos internos si existe conexión con Internet u otras redes públicas, se deberá controlar en ambos sentidos cualquier aplicación y el flujo de administración de infraestructura y se deberá proteger contra ataques de negación del servicio.	*Evaluación de controles:* El hardware y software de seguridad, así como los módulos criptográficos, están protegidos contra la intromisión o divulgación, el acceso se limita a la base de la "necesidad de conocer". Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador. *Probando que:* Los firewalls poseen por lo menos las siguientes propiedades: - Todo el tráfico de adentro hacia fuera y viceversa debe pasar por estos firewalls (esto no debe limitarse a los controles lógicos, debe reforzarse físicamente). - Sólo se permitirá el paso al tráfico autorizado, como se define en la política de seguridad local. - Los firewalls por sí mismo es inmune a la penetración. - El tráfico de intercambio en el firewall se lleva a cabo en la capa de aplicación únicamente. - La arquitectura del firewall combina las medidas de control tanto	Aplicar una herramienta para detectar las vulnerabilidades de la red. Identificar la existencia de un Firewall y sus reglas definidas actualmente. Entrevista al jefe de TI.

Cuadro 3.46 (continuación)

Matriz de pruebas DS 5.10

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS5 Garantizar la seguridad de Sistemas		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
	- La arquitectura del firewall refuerza la discontinuidad de un protocolo en la capa de transporte. - La arquitectura del firewall/IDS debe estar configurada de acuerdo a la "filosofía de arte mínimo". - La arquitectura del firewall/IDS debe desplegar sólida autenticación para la administración y sus componentes. - La arquitectura del firewall/IDS oculta la estructura de la red interna. - La arquitectura del firewall/IDS provee una auditoria de todas las comunicaciones hacia o a través del sistema del firewall y activara alarmas cuando se detecte alguna actividad sospechosa. - El host de la organización, que provee el soporte para las solicitudes de entrada al servicio e las redes públicas, permanece fuera del firewall. - La arquitectura del firewall se defiende de los ataques directos (ej. A través del monitoreo activo de la tecnología de reconocimiento de patrones y tráfico). - Todo código ejecutable se explora en busca de códigos maliciosos (ej. virus, applets dañinos) antes de introducirse.	

Cuadro 3.47

Programa de Auditoria DS 5.11

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS5 Garantizar la seguridad de Sistemas	
Contempla el control de acceso a sistemas para los diferentes usuarios, detectar, reportar y solucionar incidentes de violación de seguridad, protección de respaldos, etc.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS5.11 Intercambio de Datos Sensitivos Las políticas organizacionales deberán asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales o senderos seguros (*trusted paths*). La información sensitiva incluye información sobre administración de seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas. Para lograr esto, se pueden establecer canales confiables utilizando encripción entre usuarios, entre usuarios y sistemas y entre sistemas.	□ Acceso no autorizado a datos. □ Fuga de información confidencial de la organización. □ Posible alteración de información por canales no seguros.

Cuadro 3.48

Matriz de pruebas DS 5.11

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS5 Garantizar la seguridad de Sistemas		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS5.11 Intercambio de Datos Sensitivos Las políticas organizacionales deberán asegurar que la información de transacciones sensitivas es enviada y recibida exclusivamente a través de canales o senderos seguros. La información sensitiva incluye información sobre administración de seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas. Para lograr esto, se pueden establecer canales confiables utilizando encripción entre usuarios, entre usuarios y	*Evaluación de controles:* Existen módulos criptográficos y procedimientos de mantenimiento de llaves, si éstos son administrados centralizadamente y si son utilizados para todas las actividades de acceso externo y de transmisión. El acceso a los datos de seguridad así como la administración de la seguridad, datos de transacciones sensitivas, passwords y llaves criptográficas se limita a la base de la "necesidad de conocer". Se utilizan rutas confiables para transmitir información sensitiva no encriptada. *Probando que:* T.I. cumple con los estándares de seguridad relacionados con: - Autenticación y acceso - Estándares de administración de llaves criptográficas Existen llaves secretas para la transmisión.	Recopilar información sobre las transacciones sensitivas que se realicen. Entrevista al jefe de TI.

Cuadro 3.49

Programa de Auditoria DS 9.3

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS9 Administración de la Configuración	
Tiene que ver con el mantenimiento actualizado de inventario de hardware y software sus licencias y configuraciones.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS9.3 Revisión de Integridad de la Configuración Se deberán desarrollar y hacer cumplir políticas claras que restrinjan el uso de software personal y no licenciado. La organización deberá usar software de detección y eliminación de virus. La jefatura de TI deberá revisar periódicamente la existencia de software no autorizado en las computadoras personales de la organización. Se deberá verificar periódicamente si se está cumpliendo con los requisitos de contratos de licencia de software y de hardware.	□ Mal uso de los recursos de TI por instalación de software no autorizado. □ Ataque de virus, spyware, troyanos, etc.

Cuadro 3.50

Matriz de pruebas DS 9.3

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS9 Administración de la Configuración		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS9.3 Revisión de Integridad de la Configuración Se deberán desarrollar y hacer cumplir políticas claras que restrinjan el uso de software personal y no licenciado. La organización deberá usar software de detección y eliminación de virus. La Gerencia de TI deberá revisar periódicamente la existencia de software no autorizado en las computadoras personales de la organización. Se deberá verificar periódicamente si se está cumpliendo con los requisitos de contratos de licencia de software y de hardware.	*Evaluación de controles:* Existen procedimientos de control de cambios de software para: □ establecer y mantener una libreria de programas de aplicación con licencia. □ asegurar que la libreria de programas de aplicación con licencia sea controlada adecuadamente. □ asegurar la confiabilidad e integridad del inventario de software. □ asegurar la confiabilidad e integridad del inventario de software autorizado utilizado y revisar la existencia de software no autorizado. □ asignar responsabilidades sobre el control de software no autorizado a un miembro especifico del personal. □ registrar el uso de software no autorizado y reportar a la administración para llevar a cabo acciones correctivas. □ determinar si la administración llevó a cabo	Revisión de manuales de manejo y uso de los recursos de TI para los empleados. Solicita el inventario de software instalado en las computadoras personales. Solicitar el inventario de licencias.

Cuadro 3.50 (continuación)

Matriz de pruebas DS 9.3

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS9 Administración de la Configuración		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS9.3 Revisión de Integridad de la Configuración	*Probando que:* Para todas las computadoras personales que contengan software no autorizado se reporten violaciones y la administración lleve acciones correctivas.	Revisión de manuales de manejo y uso de los recursos de TI para los empleados. Solicita el inventario de software instalado en las computadoras personales. Solicitar el inventario de licencias.

Cuadro 3.51

Programa de Auditoria DS 11.7

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS11 Administration de Datos	
Contempla la integridad y confiabilidad de los datos, estos deben ser accedidos solo por gente autorizada.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS11.7 Chequeos de exactitud, suficiencia y autorización Los datos de transacciones, ingresados para su procesamiento (generados por personas, por sistemas o entradas de interfase) deberán estar sujetos a una variedad de controles para verificar su exactitud, suficiencia y validez. Asimismo, deberán establecerse procedimientos para asegurar que los datos de entrada sean validados y editados tan cerca del punto de origen como sea posible.	□ Ingreso de datos erróneos o alterados. □ La información en base a datos erróneos no es confiable.

Cuadro 3.52

Matriz de pruebas DS 11.7

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS11 Administración de Datos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS11.7 Chequeos de exactitud, suficiencia y autorización: Los datos de transacciones, ingresados para su procesamiento (generados por personas, por sistemas o entradas de interfase) deberán estar sujetos a una variedad de controles para verificar su exactitud, suficiencia y validez. Asimismo, deberán establecerse procedimientos para asegurar que los datos de entrada sean validados y editados tan cerca del punto de origen como sea posible.	*Evaluación de controles:* Para la entrada de datos: □ Los documentos fuente siguen un proceso de aprobación apropiada antes de su captura. □ Existe una separación de funciones apropiada entre las actividades de envío, aprobación, autorización y entrada de datos. □ Existen pistas de auditoría para identificar la fuente de entrada. □ Existen procesos de uso, mantenimiento y control de códigos de estación e IDs de operador. □ Existen rutinas de verificación para la edición de los datos capturados tan cerca del punto de origen como sea posible. □ Existen procesos apropiados de manejo de datos de entrada erróneos.	Entrevista al jefe de TI. Solicitar manuales de procedimientos para el procesamiento de datos.

Cuadro 3.52 (continuación)

Matriz de pruebas DS 11.7

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS11 Administración de Datos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS11.7 Chequeos de exactitud, suficiencia y autorización:	*Probando que:* La entrada de datos: El envío a proceso de datos de prueba (tanto transacciones correctas como erróneas) para asegurar que se lleven a cabo revisiones de precisión, suficiencia y autorización. Para transacciones seleccionadas se comparan los archivos maestros antes y después de la captura.	

Cuadro 3.53

Programa de Auditoria DS 11.8

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS11 Administracion de Datos	
Contempla la integridad y confiabilidad de los datos, estos deben ser accedidos solo por gente autorizada.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS11.8 Manejo de Errores en la Entrada de Datos La organización deberá establecer procedimientos para la corrección y reenvío de datos que hayan sido capturados erróneamente.	□ Se acepta datos no válidos para ser procesados.

Cuadro 3.54

Matriz de pruebas DS 11.8

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS11 Administración de Datos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS11.8 Manejo de Errores en la Entrada de Datos La organización deberá establecer procedimientos para la corrección y reenvío de datos que hayan sido capturados erróneamente.	*Evaluación de controles:* Para el procesamiento de datos: Los programas contienen rutinas de prevención, detección y corrección de errores: □ los programas deben probar las entradas en cuanto a errores (por ejemplo, validación y edición), □ los programas deben validar todas las transacciones contra una lista maestra, □ los programas deben rechazar la anulación de condiciones de error. Los procesos de manejo de errores incluyen: La corrección de errores y reenvío de la transacción debe ser aprobado. Existen procedimientos por escrito para la corrección y reenvio de datos con errores incluyendo una solución que no afecte su reprocesamiento. Las transacciones reenviadas son procesadas exactamente como fueron procesadas originalmente. La responsabilidad de la corrección de errores reside dentro de la	Entrevista al jefe de TI. Solicitar manuales de procedimientos para el procesamiento de datos.

Cuadro 3.54 (continuación)

Matriz de pruebas DS 11.8

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS11 Administración de Datos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS11.8 Manejo de Errores en la Entrada de Datos	*Probando que:* El procesamiento de datos: Se envían datos de prueba (tanto transacciones correctas como erróneas) para asegurar que se llevan a cabo la validación, autenticación y edición de procesamiento de datos tan cerca del punto de origen como sea posible. El proceso de manejo de errores es llevado a cabo de acuerdo con los procedimientos y controles establecidos. Se llevan a cabo la retención, solución y revisión apropiada de la integridad en el manejo de errores y que éstas funcionan adecuadamente. Los procedimientos y acciones del manejo de errores cumplen con los procedimientos y controles establecidos.	Entrevista al jefe de TI. Solicitar manuales de procedimientos para el procesamiento de datos.

Cuadro 3.55

Programa de Auditoria DS 11.9

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS11 Administracion de Datos	
Contempla la integridad y confiabilidad de los datos, estos deben ser accedidos solo por gente autorizada.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS11.9 Integridad de procesamiento de datos La organización deberá establecer procedimientos para el procesamiento de datos que aseguren que la segregación de funciones sea mantenida y que el trabajo realizado sea verificado rutinariamente. Los procedimientos deberán asegurar que se establezcan controles de actualización adecuados como totales de control "corrida a corrida" y controles de actualización de archivos maestros.	□ Datos mal procesados.

Cuadro 3.56

Matriz de pruebas DS 11.9

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS11 Administración de Datos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS11.9 Integridad de procesamiento de datos: La organización deberá establecer procedimientos para el procesamiento de datos que aseguren que la segregación de funciones sea mantenida y que el trabajo realizado sea verificado rutinariamente. Los procedimientos deberán asegurar que se establezcan controles de actualización adecuados como totales de control "corrida a corrida" y controles de actualización de archivos maestros.	*Evaluación de controles:* Para el procesamiento de datos: Los programas contienen rutinas de prevención, detección y corrección de errores: □ los programas deben probar las entradas en cuanto a errores □ los programas deben validar todas las transacciones contra una lista maestra. □ los programas deben rechazar la anulación de condiciones de error. Los procesos de manejo de errores incluyen: □ La corrección de errores y reenvio de la transacción debe ser aprobada. □ Existen bitácoras de los programas ejecutados y las transacciones procesadas/rechazadas para pistas de auditoria. □ Las tablas utilizadas en la validación son revisadas frecuentemente.	Entrevista al jefe de TI. Solicitar manuales de procedimientos para el procesamiento de datos.

Cuadro 3.56 (continuación)

Matriz de pruebas DS 11.9

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS11 Administración de Datos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS11.9 Integridad de procesamiento de datos:	□ Existe un grupo de control para monitorear las actividades de entrada e investigar los eventos no-estándar, asi como balancear las cuentas de registros y totales de control para todos los datos procesados. □ Las transacciones reenviadas son procesadas exactamente como fueron procesadas originalmente. □ La responsabilidad de la corrección de errores reside dentro de la función de envío original. *Probando que:* El procesamiento de datos: □ Se utilizan efectivamente los totales de control corrida -a-corrida y los controles de actualización de archivos maestros. □ Existen procedimientos por escrito para la corrección y reenvio de datos con errores incluyendo una solución que no afecte su reprocesamiento.	

Cuadro 3.57

Programa de Auditoria DS 11.10

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS11 Administracion de Datos	
Contempla la integridad y confiabilidad de los datos, estos deben ser accedidos solo por gente autorizada.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS11.10 Validación y Edición de procesamiento de Datos La organización deberá establecer procedimientos para asegurar que la validación, autenticación y edición del procesamiento sean llevadas a cabo tan cerca del punto de origen como sea posible. Cuando se utilicen sistemas de Inteligencia Artificial, dichos sistemas serán ubica dos en una infraestructura de control interactiva con operadores humanos para asegurar que las decisiones vitales son aprobadas.	□ Ingreso de datos erróneos o alterados. □ La información en base a datos erróneos no es confiable.

Cuadro 3.58

Matriz de pruebas DS 11.10

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS11 Administración de Datos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS11.10 Validación y Edición de procesamiento de Datos La organización deberá establecer procedimientos para asegurar que la validación, autenticación y edición del procesamiento sean llevadas a cabo tan cerca del punto de origen como sea posible. Cuando se utilicen sistemas de Inteligencia Artificial, dichos sistemas serán ubicados en una infraestructura de control interactiva con operadores humanos para asegurar que las decisiones vitales son	*Evaluación de controles:* Para el procesamiento de datos: Los programas contienen rutinas de prevención, detección y corrección de errores: □ los programas deben probar las entradas en cuanto a errores (por ejemplo, validación y edición). Los procesos de manejo de errores incluyen: Los sistemas de Inteligencia Artificial están colocados en un marco referencial de control interactivo con operadores humanos para aseguran que las decisiones importantes se aprueben. *Probando que:* El procesamiento de datos: Se envían datos de prueba para asegurar que se llevan a cabo la validación, autenticación y edición de procesamiento	Entrevista al jefe de T.I. Solicitar manuales de procedimientos para el procesamiento de datos.

Cuadro 3.59

Programa de Auditoria DS 11.23

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS11 Administracion de Datos	
Contempla la integridad y confiabilidad de los datos, estos deben ser accedidos solo por gente autorizada.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS11.23 Respaldos y Restauraciones La jefatura deberá implementar una estrategia apropiada de respaldo y recuperación para asegurar que ésta incluya una revisión de los requerimientos del negocio, así como el desarrollo, implementación, prueba y documentación del plan de recuperación. Se deberán establecer procedimientos para asegurar que los respaldos satisfagan los requerimientos mencionados anteriormente.	□ Plan de contingencia no efectivo no eficiente. □ Daño en los dispositivos de respaldo por el medioambiente inadecuado para almacenamiento.

Cuadro 3.60

Matriz de pruebas DS 11.23

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS11 Administración de Datos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS11.23 Respaldos y Restauraciones El vicerrectorado deberá implementar una estrategia apropiada de respaldo y recuperación para asegurar que ésta incluya una revisión de los requerimientos del negocio, así como el desarrollo, implementación, prueba y documentación del plan de recuperación. Se deberán establecer procedimientos para asegurar que los respaldos satisfagan los requerimientos mencionados anteriormente.	*Evaluación de controles:* Existen estrategias de respaldo y restauración de medios. Los respaldos de medios se llevan a cabo de acuerdo con la estrategia de respaldos y si la utilidad de los respaldos es verificada regularmente. Los respaldos de medios son almacenados con seguridad y si las localidades de almacenamiento son revisadas periódicamente en cuanto a la seguridad de sus acceso físico y a la seguridad de los archivos de datos y otros elementos. *Probando que:* Confirmar la creación e integridad de los respaldos en asociación con el procesamiento normal, así como para los requerimientos del plan de	Entrevista al jefe de T.I. Aplicación de lista de chequeo al jefe de TI.

Cuadro 3.61

Programa de Auditoria DS 11.24

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS11 Administracion de Datos	
Contempla la integridad y confiabilidad de los datos, estos deben ser accedidos solo por gente autorizada.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS11.24 Funciones de Respaldo Deberán establecerse procedimientos para asegurar que los respaldos sean realizados de acuerdo con la estrategia de respaldo definida, y que las copias de respaldo sean verificadas regularmente.	□ Pérdida o daño de la información. □ Daño en los dispositivos de respaldo por el medioambiente inadecuado para almacenamiento

Cuadro 3.62

Matriz de pruebas DS 11.24

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS11 Administración de Datos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS11.24 Funciones de Respaldo Deberán establecerse procedimientos para asegurar que los respaldos sean realizados de acuerdo con la estrategia de respaldo definida, y que las copias de respaldo sean verificadas regularmente.	*Evaluación de controles:* Los respaldos de medios se llevan a cabo de acuerdo con la estrategia de respaldos y si la utilidad de los respaldos es verificada regularmente. *Probando que:* Revisar los procedimientos de creación de respaldos para asegurar la existencia de datos suficientes en caso de desastre.	Entrevista al jefe de T.I. Aplicación de lista de chequeo al jefe de TI.

Cuadro 3.63

Programa de Auditoria DS 11.27

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS11 Administracion de Datos	
Contempla la integridad y confiabilidad de los datos, estos deben ser accedidos solo por gente autorizada.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS11.27 Protección de mensajes sensitivos Con respecto a la transmisión de datos a través de Internet u otra red pública, la jefatura deberá definir e implementar procedimientos y protocolos que deben ser utilizados para el aseguramiento de la integridad, confidencialidad y "no negación/rechazo" de mensajes sensitivos.	□ Intercepción o alteración de mensajes sensibles.

Cuadro 3.64

Matriz de pruebas DS 11.27

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS11 Administración de Datos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS11.27 Protección de mensajes sensitivos: Con respecto a la transmisión de datos a través de Internet u otra red pública, la jefatura deberá definir e implementar procedimientos y protocolos que deben ser utilizados para el aseguramiento de la integridad, confidencialidad y "no negación/rechazo" de mensajes sensitivos.	*Evaluación de controles:* Para las salidas, interfaces y distribución: Existen pistas de auditoría para facilitar el seguimiento del procesamiento de transacciones y la reconciliación de datos alterados. Existe una definición clara sobre aspectos de seguridad durante las salidas, interfaces y distribución. Las fallas en seguridad durante cualquier fase son comunicadas a la administración, se llevan a cabo acciones correctivas sobre ellas y son reflejadas apropiadamente en nuevos procedimientos. Para la autenticación e integridad de información: La integridad de los archivos de datos se verifica periódicamente. La firma electrónica o la certificación se utilizan para verificar la integridad y autenticidad de los	Entrevista al jefe de T.I. Solicitar manuales de procedimientos para el procesamiento de datos.

Cuadro 3.64 (continuación)

Matriz de pruebas DS 11.27

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS11 Administración de Datos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS11.27 Protección de mensajes sensitivos:	*Probando que:* La Salida, Interface y Distribución de Datos: Las pistas de auditoria son proporcionadas para facilitar el seguimiento del procesamiento de transacciones en la reconciliación de datos confusos o erróneos. Los reportes de salida son revisados en cuanto a su precisión por parte del proveedor y los usuarios relevantes. Existen la retención, solución y revisión apropiada de la integridad en el manejo de errores y que éstas funcionan adecuadamente. Existe una protección adecuada de información sensitiva durante la transmisión y transporte en cuanto a accesos y modificaciones no autorizadas. Para la integridad y autenticación de la información: Existen protecciones adecuadas para asegurar la integridad, confidencialidad y no rechazo de los mensajes sensitivos	

Cuadro 3.65

Programa de Auditoria DS 11.29

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS11 Administracion de Datos	
Contempla la integridad y confiabilidad de los datos, estos deben ser accedidos solo por gente autorizada.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS11.29 Integridad de transacciones electrónicas Tomando en consideración que las fronteras tradicionales de tiempo y de geografía son menos precisas y confiables, la jefatura deberá definir e implementar apropiados procedimientos y prácticas para transacciones electrónicas que sean sensitivas y críticas para la Organización, que permitan asegurar su integridad y autenticidad de: - atomicidad (unidad de trabajo indivisible, todas sus acciones tienen éxito o todas ellas fallan) - consistencia (si la transacción no logra alcanzar un estado final estable, deberá regresar al sistema a su estado inicial); - aislamiento (el comportamiento de una transacción no es afectado por otras transacciones que se ejecutan concurrentemente); y - durabilidad (los efectos de una transacción son permanentes después que concluye su proceso, los cambios que origina deben sobrevivir a fallas de	□ Intercepción o alteración de las transacciones electrónicas.

Cuadro 3.66

Matriz de pruebas DS 11.29

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS11 Administración de Datos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS11.29 Integridad de transacciones electrónicas Tomando en consideración que las fronteras tradicionales de tiempo y de geografía son menos precisas y confiables, la jefatura deberá definir e implementar apropiados procedimientos y prácticas para transacciones electrónicas que sean sensitivas y críticas para la Organización, que permitan asegurar su integridad y autenticidad de: - atomicidad - consistencia;	*Evaluación de controles:* Para las salidas, interfaces y distribución: Existen pistas de auditoría para facilitar el seguimiento del procesamiento de transacciones y la reconciliación de datos alterados. Existe una definición clara sobre aspectos de seguridad durante las salidas, interfaces y distribución. Las fallas en seguridad durante cualquier fase son comunicadas a la administración, se llevan a cabo acciones correctivas sobre ellas y son reflejadas apropiadamente en nuevos procedimientos. Para la autenticación e integridad de información: La integridad de los archivos de datos se verifica periódicamente. La firma electrónica o la certificación se utilizan para verificar la integridad y autenticidad de los	Entrevista al jefe de TI. Entrevista a los usuarios de las aplicaciones que implican transacciones electrónicas.

Cuadro 3.66 (continuación)

Matriz de pruebas DS 11.29

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS11 Administración de Datos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS11.29 Integridad de transacciones electrónicas - aislamiento (el comportamiento de una transacción no es afectado por otras transacciones que se ejecutan concurrentemente); y - durabilidad (los efectos de una transacción son permanentes después que concluye su proceso, los cambios que origina deben sobrevivir a fallas de sistema).	*Probando que:* La Salida, Interface y Distribución de Datos: Existen la retención, solución y revisión apropiada de la integridad en el manejo de errores y que éstas funcionan adecuadamente. Los procedimientos y acciones de manejo de errores cumplen con las políticas y controles establecidos. Existe la protección adecuada para la información sensible durante la transmisión y transporte contra los accesos no autorizados y las modificaciones. Para la integridad y autenticación de la información: Existen protecciones adecuadas para asegurar la integridad, confidencialidad y no rechazo de los mensajes sensitivos transmitidos sobre Internet o cualquier otra red pública.	

Cuadro 3.67

Programa de Auditoria DS 12.2

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS12 Administración del Ambiente Físico	
Seguridades físicas del área de Tecnología de Información incluye cableado de red, equipos de comunicación, computadores, periféricos y electricidad.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS12.2 Medidas de Seguridad Física Deberán establecerse medidas apropiadas de seguridad física y medidas de control de acceso para las instalaciones de tecnología de información incluyendo el uso de dispositivos de información off-site en conformidad con la política general de seguridad. La seguridad física y los controles de acceso deben abarcar no sólo el área que contenga el hardware del sistema sino también las ubicaciones del cableado usado para conectar elementos del sistema, servicios de soporte (como la energía eléctrica), medios de respaldo y demás elementos requeridos para la operación del sistema. El acceso deberá restringirse a las personas que hayan sido autorizadas. Cuando los recursos de tecnología de información estén ubicados en áreas públicas, deberán estar debidamente protegidos para impedir o para prevenir pérdidas o daños por robo o por vandalismo.	□ Ingreso de personas no autorizadas a áreas restringidas de procesamiento de datos. □ Robo, pérdida o daño de equipos o datos.

Cuadro 3.68

Matriz de pruebas DS 12.2

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS12 Administración del Ambiente Físico		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS12.2 Medidas de Seguridad Física Deberán establecerse medidas apropiadas de seguridad física y medidas de control de acceso para las instalaciones de tecnología de información incluyendo el uso de dispositivos de información offsite en conformidad con la política general de seguridad.	*Evaluación de controles:* La localización de las instalaciones no es obvia externamente, se encuentra en el área u organización menos accesible, y si el acceso es limitado al menor número de personas. Los procedimientos de acceso lógico y físico son suficientes, incluyendo perfiles de seguridad de acceso para empleados, proveedores, equipo y personal de mantenimiento de las instalaciones. Los procedimientos y prácticas de administración de llave y lectora de tarjetas son adecuados, incluyendo la actualización y revisión continua tomando como base una "menor necesidad de acceso". Las políticas de acceso y autorización de entrada/salida, escolta, registro, pases temporales requeridos, cámaras de vigilancia son apropiadas para todas las áreas y especialmente para las áreas más sensibles. Las medidas de control de seguridad y acceso incluyen a los	Entrevista al jefe de TI. Aplicación de lista de chequeo sobre seguridad física de TI. Observaciones in situ.

Cuadro 3.68 (continuación)

Matriz de pruebas DS 12.2

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS12 Administración del Ambiente Físico		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS12.2 Medidas de Seguridad Física La seguridad física y los controles de acceso deben abarcar no sólo el área que contenga el hardware del sistema sino también las ubicaciones del cableado usado para conectar elementos del sistema, servicios de soporte (como la energía eléctrica), medios de respaldo y demás elementos requeridos para la operación del sistema. El acceso deberá restringirse a las personas que hayan sido autorizadas. Cuando los recursos de tecnología de información estén ubicados en áreas públicas, deberán estar debidamente protegidos para impedir o para prevenir pérdidas o daños por robo o por	Se lleva a cabo una revisión de los registros de visitantes, asignación de pases, escolta, persona responsable del visitante, bitácora para asegurar tanto los registros de entradas como de salidas y el conocimiento de la recepcionista con respecto a los procedimientos de seguridad. Existe una revisión del proceso de alarma al ocurrir una violación a la seguridad, que incluya: □ definición de la prioridad de la alarma (por ejemplo, apertura de la puerta por parte de una persona armada que ha entrado en las instalaciones) □ escenarios de respuesta para cada alarma de prioridad □ responsabilidades del personal interno versus personal de seguridad local o proveedores □ interacción con las autoridades locales □ revisión del simulacro de alarma más reciente La organización es responsable del acceso físico dentro de la función de servicios de información,	

Cuadro 3.68 (continuación)

Matriz de pruebas DS 12.2

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS12 Administración del Ambiente Físico		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS12.2 Medidas de Seguridad Física	□ Desarrollo, mantenimiento y revisiones continuas de políticas y procedimientos de seguridad. □ Establecimiento de relaciones con proveedores relacionados con la seguridad. • Contacto con la administración de las instalaciones en cuanto a problemas de tecnología relacionados con seguridad. • Coordinación del entrenamiento y conciencia sobre seguridad para la organización. • Coordinación de actividades que afecten en control de acceso lógico vía aplicaciones centralizadas y software de sistema operativo. • Proporcionar entrenamiento y crear conciencia de seguridad no sólo dentro de la función de servicios de información, sino para los servicios de usuarios. *Probando que:* Los armarios cableados están físicamente protegidos con el acceso posible autorizado y el cableado se encuentra bajo tierra o conductos protegidos tanto como sea posible. La bitácora de visitantes sigue apropiadamente los procedimientos de seguridad. Existen los procedimientos de identificación requeridos para cualquier acceso dentro o fuera vía observación.	

Cuadro 3.68 (continuación)

Matriz de pruebas DS 12.2

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS12 Administración del Ambiente Físico		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS12.2 Medidas de Seguridad Física	Las puertas, ventanas, elevadores, ventilas y ductos o cualquier otro modo de acceso están identificados. El site computacional está separado, cerrado y asegurado y es accesado únicamente por personal de operaciones y gente de mantenimiento tomando como base un "acceso necesario". Los planes físicos son actualizados a medida que cambian la configuración, el ambiente y las instalaciones. No se almacenan útiles peligrosos. Existe el seguimiento de auditoria de control de acceso sobre software de seguridad o reportes clave de administración. Se llevan a cabo verificaciones de suficiencia de administración clave de acceso. Se otorga una educación en seguridad física y conciencia de seguridad. Existe una cobertura y experiencia de seguros para los gastos asociados con algún evento de seguridad, pérdida del negocio y gastos para recuperar la	

Cuadro 3.69

Programa de Auditoria DS 12.4

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS12 Administración del Ambiente Físico	
Seguridades físicas del área de Tecnología de Información incluye cableado de red, equipos de comunicación, computadores, periféricos y electricidad.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS12.4 Protección contra factores ambientales La jefatura de la función de servicios de información deberá asegurar que se establezcan y mantengan las suficientes medidas para la protección contra los factores ambientales (por ejemplo, fuego, polvo, electricidad, calor o humedad excesivos). Deberán instalarse equipo y dispositivos especializados para monitorear y controlar el ambiente.	□ Pérdida o daño de equipos o datos.

Cuadro 3.70

Matriz de pruebas DS 12.4

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS12 Administración del Ambiente Físico		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS12.4 Protección contra factores ambientales: La jefatura de la función de servicios de información deberá asegurar que se establezcan y mantengan las suficientes medidas para la protección contra los factores ambientales (por ejemplo, fuego, polvo, electricidad, calor o humedad excesivos). Deberán instalarse equipo y dispositivos especializados para monitorear y controlar el ambiente.	*Evaluación de controles:* Se lleva a cabo una revisión de los procedimientos de aviso contra incendio, cambios de clima, problemas eléctricos y procedimientos de alarma, así como las respuestas esperadas en los distintos escenarios para los diferentes niveles de emergencias ambientales. Se lleva a cabo una revisión de los procedimientos de control de aire acondicionado, ventilación, humedad y las respuestas esperadas en los distintos escenarios de pérdida o extremos no anticipados. *Probando que:* Los planes físicos son actualizados a medida que cambian la configuración, el ambiente y las instalaciones. Los registros y el equipo de monitoreo ambiental y de seguridad -debajo, en, sobre, y alrededor – son mantenidos.	Entrevista al jefe de TI. Aplicación de la lista de chequeo sobre seguridad física de TI. Observaciones in situ.

Cuadro 3.71

Programa de Auditoria DS 12.5

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE	
DS12 Administración del Ambiente Físico	
Seguridades físicas del área de Tecnología de Información incluye cableado de red, equipos de comunicación, computadores, periféricos y electricidad.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
DS12.5 Administración de Instalaciones Físicas La jefatura deberá evaluar regularmente la necesidad de contar con generadores y baterías de suministro ininterrumpido de energía (UPS) para las aplicaciones críticas de tecnología de información, con el fin de protegerse contra fallas y fluctuaciones de energía. Cuando sea justificable, deberá instalarse el equipo más apropiado.	□ Falla de energía eléctrica. □ Falla o daño de equipos. □ Falla de los servicios de red y comunicaciones.

Cuadro 3.72

Matriz de pruebas DS 12.5

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
DS12 Administración del Ambiente Físico		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
DS12.5 Administración de Instalaciones Físicas La jefatura deberá evaluar regularmente la necesidad de contar con generadores y baterías de suministro ininterrumpido de energía (UPS) para las aplicaciones críticas de tecnología de información, con el fin de protegerse contra fallas y fluctuaciones de energía. Cuando sea justificable, deberá instalarse el equipo más apropiado.	*Evaluación de controles:* Existen elementos de infraestructura específicos alternativos necesarios para implementar seguridad: - Fuente de poder ininterrumpida UPS. *Probando que:* Prueba de UPS y verificar que los resultados cumplan con los requerimientos operacionales de capacidad para sostener las actividades críticas de procesamientos de datos.	Entrevista al jefe de TI. Solicitud de documentación técnica de equipos UPS.

3.4 Procesos del Dominio de Monitoreo y Evaluación.

Cuadro 3.73

Programa de Auditoria ME 3.1

DOMINIO: MONITOREO y EVALUACION	
ME3 Garantizar el cumplimiento con requerimientos externos	
Garantizar el cumplimiento de las leyes, regulaciones y requerimientos contractuales.	
OBJETIVO DE CONTROL DETALLADO	**FACTORES DE RIESGO**
ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales La jefatura deberá asegurar el cumplimiento de las regulaciones sobre privacidad, propiedad intelectual, flujo de datos a entes externos y regulaciones de criptografía aplicables a las prácticas de tecnología de información de la organización. La jefatura deberá asegurar que se establezcan contratos formales para que existan acuerdos entre socios comerciales sobre procesos de comunicación, así como sobre estándares de mensajes transaccionales, seguridad y almacenamiento de datos. Cuando se realicen operaciones de intercambio en Internet, la gerencia deberá imponer adecuados controles para asegurar el cumplimiento de leyes locales y de clientes sobre bases internacionales	□ Pérdida de la confidencialidad, integridad y confiabilidad de los datos manejados por la empresa. □ Flujo de información privada hacia destinos no autorizados. □ Los mensajes pueden estar siendo interceptados por terceros, y la información susceptible de cambio o divulgación indeseada. □ Las debilidades en el contenido de los contratos con los proveedores de servicios pueden acarrear en problemas legales posteriores si se cae en incidentes de seguridad.

Cuadro 3.74

Matriz de pruebas M 3.1

ME3 Garantizar el cumplimiento con requerimientos externos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales La jefatura deberá asegurar el cumplimiento de las regulaciones sobre privacidad, propiedad intelectual, flujo de datos a entes externos y regulaciones de criptografía aplicables a las prácticas de tecnología de información de la organización. La jefatura deberá asegurar que se establezcan contratos formales para que existan acuerdos entre socios comerciales sobre procesos de comunicación, así como sobre estándares de mensajes transaccionales, seguridad y almacenamiento de datos.	*Evaluación de controles* Los procedimientos de seguridad van de acuerdo con todos los requerimientos legales y si éstos están siendo tomados en cuenta adecuadamente, incluyendo: - protección con "passwords" o contraseñas y software para limitar el acceso - procedimientos de autorización - medidas de seguridad de terminales - medidas de encriptación de datos - controles de Firewalls - protección contra virus - seguimiento oportuno de reportes de violaciones Existen políticas y procedimientos para: - Asegurar las acciones correctivas apropiadas relacionadas con la revisión oportuna de los requerimientos externos y si existen procedimientos para asegurar un cumplimiento continuo.	Se solicita manual de procedimientos Entrevista al jefe de área, y colaboradores de TI, para aplicar revisión del listado.

Cuadro 3.74 (continuación)

Matriz de pruebas M 3.7

DOMINIO: MONITOREO y EVALUACION		
ME3 Garantizar el cumplimiento con requerimientos externos		
OBJETIVO DE CONTROL DETALLADO	**REVISION A TRAVES DE:**	**DESCRIPCION DE LA PRUEBA**
ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales Cuando se realicen operaciones de intercambio en Internet, la jefatura deberá imponer adecuados controles para asegurar el cumplimiento de leyes locales y de clientes sobre bases internacionales.	- Coordinar la revisión de los requerimientos externos, con el fin de asegurar que se aplican oportunamente las acciones correctivas que garantizan el cumplimiento de los requerimientos externos. - Monitorear el cumplimiento de las leyes y regulaciones aplicables de seguridad y salud. - Proporcionar la dirección/enfoque adecuados sobre privacidad de tal manera que todos los requerimientos legales caigan dentro de este alcance. *Probando que:* En donde se hayan impuesto límites regulatorios a los tipos de encriptación que pueden ser utilizados, la encriptación aplicada cumpla con las regulaciones. En donde las regulaciones o procedimientos internos requieran la protección y/o encriptación especial de ciertos elementos de datos dicha protección/encriptación sea proporcionada a estos datos. Los datos transmitidos a través de las fronteras internacionales no violan las leyes de exportación. Los contratos existentes con los proveedores de comercio electrónico consideren adecuadamente los requerimientos	

3.5 Cronograma de la Auditoria

Actividad / Semana	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Conocimiento de la Situación Actual de la Red Informática	■													
Evaluación e identificación de riesgos		■												
Elaboración del Plan de Auditoría			■											
Selección de los Procesos COBIT aplicables a la Auditoría			■											
Puesta en marcha del Plan de Auditoría				■	■	■								
Elaboración del Programa de Auditoría				■	■									
Elaboración de Matriz de Pruebas				■	■									
Recolección de documentación: manuales de procedimientos, funciones y políticas						■								
Evaluación y Análisis de las pruebas realizadas							■	■	■	■				
Elaboración del Informe Preliminar											■	■		
Discusión del Informe Preliminar													■	
Elaboración del Informe Final														■

Capitulo 4

4.1 Análisis de resultados

Terminada la fase de toma de pruebas se aplicará una evaluación del cumplimiento de las mismas para cada uno de los objetivos de control detallados permitiendo al final obtener el nivel actual de la gestión de seguridad que se maneja en la universidad. En base a esto se presentará la situación actual de los objetivos de control que cumplen los requerimientos y sobre los que no cumplen se harán recomendaciones en el informe final.[13]

Evaluación de Resultados

Cuadro 4.1

Evaluación de pruebas PO2.3

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
PO 2 Definir la Arquitectura de la Información				
PO 2.3 Esquema de Clasificación de datos				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Se cuenta con un esquema de clasificación de datos en operación que indique que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido. *Probando que:* Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema.	Entrevista al jefe de TI. Revisión de manuales de procedimientos.	NO EFECTIVO		Crear un procedimiento para la clasificación y responsabilidad de datos según la criticidad e importancia.

Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad. El esquema de clasificación debe incluir criterios para administrar el intercambio de información entre organizaciones, teniendo en cuenta tanto la seguridad y el cumplimiento como la legislación relevante.				

Cuadro 4.2

Evaluación de pruebas PO 4.6

DOMINIO: PLANEACION Y ORGANIZACIÓN				
PO4 Definición de los proceso, organización y las relaciones de TI				
PO4.6 Establecimiento de Roles y Responsabilidades				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Existen políticas que determinen los roles y responsabilidades para todo el personal dentro de la organización con respecto a sistemas de información, control interno y seguridad. La jefatura de TI en cuenca ha asignado formalmente la responsabilidad a lo largo de toda la organización para la formulación de políticas y procedimientos de control interno y seguridad (tanto lógica como física) a un oficial de seguridad. El oficial de seguridad de la información comprende adecuadamente sus funciones y responsabilidades y si éstas han mostrado consistencia con respecto a	Revisión del documento de descripción de funciones. Entrevista al jefe de TI.	NO EFECTIVO	Descripción de Funciones del Personal del Departamento de TI.	No existen documentos específicos sobre responsabilidades de seguridad, pero se entiende que la responsabilidad la tiene el jefe de TI

la política de seguridad de la información de la organización. Las políticas de seguridad de la organización definen claramente las responsabilidades sobre la seguridad de la información que cada propietario de los activos (por ejemplo, usuarios, administración y administradores de seguridad) debe llevar a cabo. *Probando que:* El personal de seguridad revisa los sistemas operativos y los sistemas de aplicación esenciales.				

Cuadro 4.3

Evaluación de pruebas PO 4.11

DOMINIO: PLANEACION Y ORGANIZACIÓN				
PO4 Definición de los proceso, organización y las relaciones de TI				
PO4.11 Segregación de Funciones				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Existen políticas y procedimientos que describan las prácticas de superación para asegurar que las funciones y responsabilidades sean ejercidas apropiadamente y que todo el personal cuente con suficiente autoridad y recursos para llevar a cabo sus funciones y responsabilidades. Existe una segregación de funciones entre los siguientes pares de unidades: - Desarrollo y mantenimiento de sistemas - Operaciones y control de datos - Desarrollo y operaciones de	Revisión del documento de descripción de Funciones del Departamento de Sistemas. Entrevista al jefe de TI.	EFECTIVO	Descripción de Funciones del Personal del Departamento de TI.	

sistemas - Desarrollo/Mantenimiento de sistemas y seguridad de la información. - Operaciones y usuarios - Operaciones y seguridad de la información Probando que: Las descripciones de los puestos de trabajo tienen claramente delimitada tanto la autoridad como la responsabilidad. La naturaleza y el alcance de la suficiencia de la segregación de funciones deseadas y de las limitaciones de funciones dentro de TI.				

Cuadro 4.4

Evaluación de pruebas PO 6.4

DOMINIO: PLANEACION Y ORGANIZACIÓN				
PO6 Comunicación de las aspiraciones y la dirección de la Gerencia				
PO6.4 Implantación de políticas de TI				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Existen procedimientos apropiados para asegurar que el personal comprende las políticas y procedimientos implementados, y que se cumple con dichas políticas y procedimientos. La administración de la función de servicios de información asegura que la filosofía de calidad, las políticas y objetivos sean comprendidas, implementadas y mantienen a todos los niveles de la función de servicios de información. Probando que:	Entrevista al jefe de TI. Revisión del Documento Políticas de TI.	NO EFECTIVO	Documento Corporativo de Políticas de TI.	Establecer procedimientos de evaluación a usuarios, en cuanto a lo que tiene que ver con el cumplimiento de políticas de seguridad, y otros procedimientos relativos a controles.

Los esfuerzos de reforzamiento de la administración con respecto a los estándares, directivas, políticas y procedimientos relacionados con su ambiente de control interno están asegurando su cumplimiento a través de toda la organización.				

Cuadro 4.5

Evaluación de pruebas PO 6.11

DOMINIO: PLANEACION Y ORGANIZACIÓN				
PO6 Comunicación de las aspiraciones y la dirección de la Gerencia				
PO6.5 Comunicación de los objetivos y la dirección de TI				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Las políticas y procedimientos de la organización crean un marco referencial y un programa de concientización, con atención especial a la TI, propiciando un ambiente de control positivo y considerando aspectos como: - Integridad - Valores éticos - Código de conducta - Seguridad y control interno - Competencia del personal - Filosofía y estilo operativo de la administración - Responsabilidad, atención y dirección proporcionadas por el	Entrevista al jefe de TI. Revisión del Documento Políticas de TI.	EFECTIVO	Documento Corporativo de Políticas de TI.	

consejo directivo o su equivalente *Probando que:* Los empleados han recibido el código de conducta y lo comprenden. Miembros seleccionados de la administración están involucrados y comprenden el contenido de las actividades de seguridad y control interno (pj. reportes de excepción, reconciliaciones, comparaciones, etc.) bajo su responsabilidad. Las funciones individuales, las responsabilidades y líneas de autoridad se comunican claramente y se comprenden en todos los niveles de la organización.				

Cuadro 4.6

Evaluación de pruebas PO7.4

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS7 Administrar los Recursos Humanos de TI				
PO 7.4 Entrenamiento del Personal de TI				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: El entrenamiento de los empleados incluye un conocimiento y conciencia sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus. El refuerzo a las políticas relacionadas con cargos sensitivos, incluyen: - Se les pide a los empleados en puestos sensitivos que permanezcan alejados de la organización durante un periodo adecuado de tiempo cada año calendario (periodo de vacaciones; durante éste tiempo su user ID es suspendido; y la persona	Revisión de manuales de manejo y uso de los recursos de TI para los empleados. Entrevista al jefe de TI.	NO EFECTIVO	Documento de Políticas de TI.	Establecer programas de concientización regulares sobre la seguridad de los datos tanto personales como de los sistemas que se manejan en el hotel.

que remplaza a el empleado es instruido en el sentido que debe notificar a la administración si nota cualquier anormalidad relacionada con la seguridad). - La rotación de personal involucrado en actividades sensitivas, sin previa notificación, se realiza de tiempo en tiempo. *Probando que:* Las responsabilidades de los empleados con respecto a la confidencialidad, integridad, disponibilidad, confiabilidad y seguridad de todos los recursos de TI son comunicadas continuamente. Existen programas de entrenamiento vigentes para concientizar a los nuevos y antiguos empleados en seguridad.				

Cuadro 4.7

Evaluación de pruebas PO 9.3

DOMINIO: PLANEACION Y ORGANIZACIÓN				
PO9 Evaluar y Administrar los riesgos de TI				
PO9.3 Identificación de Eventos				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Los objetivos de toda la organización están incluidos en el proceso de identificación de riesgos. Se incluyen técnicas de probabilidad, frecuencia y análisis de amenazas en la identificación de riesgos. Existe un enfoque cuantitativo y/o cualitativo (o combinado) formal para la identificación y medición de riesgos, amenazas y exposiciones. *Probando que:* La administración comprende los factores relacionados con los riesgos	Recopilación de planes de contingencia. Entrevista con el jefe de TI.	NO EFECTIVO	Planes de Contingencia existentes.	Establecer procedimientos para identificar los recursos críticos de la empresa, los riesgos potenciales, y la incidencia que estos producirían en el cumplimiento de los objetivos de la empresa.

y la probabilidad de amenazas. Los reportes emitidos al Vicerrectorado para su revisión y acuerdo con los riesgos identificados y utilización en el monitoreo de actividades de reducción de riesgos sean oportunos.				

Cuadro 4.8

Evaluación de pruebas PO 9.5

DOMINIO: PLANEACION Y ORGANIZACIÓN				
PO9 Evaluar y Administrar los riesgos de TI				
PO9.5 Respuesta a Riesgos				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: – Existen procedimientos para el monitoreo y el mejoramiento continuos de la evaluación de riesgos y procesos para la creación de controles que mitiguen los riesgos. – El plan de acción contra riesgos es utilizado en la implementación de medidas apropiadas para mitigar los riesgos, amenazas y exposiciones. *Probando que:*	Revisión de los planes de Contingencia.	NO EFECTIVO	Planes de Contingencia existentes.	Elaborar planes de Contingencia para cada uno de los recursos críticos antes identificados, y sus potenciales riesgos. Actualizar los planes de Contingencia existentes.

El plan de acción contra riesgos es actual e incluye controles económicos y medidas de seguridad para mitigar la exposición al riesgo. Se han priorizado los riesgos desde el más alto hasta el más bajo y existe una respuesta apropiada para cada riesgo.				

Cuadro 4.9

Evaluación de pruebas AI3.2

DOMINIO: ADQUISICION E IMPLEMENTACION				
AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica				
AI3.2 Protección y Disponibilidad del recurso de infraestructura.				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Existen políticas y procedimientos asegurando que: - La posibilidad de acceso al software del sistema y con ella, la posibilidad de interrumpir los sistemas de información operativa está limitada. - La preparación, instalación y mantenimiento del software del sistema no amenaza la seguridad de los datos y programas almacenados. - Se seleccionan parámetros del software del sistema para asegurar la integridad de los datos y programas almacenados en el sistema. *Probando que:*	Entrevista al jefe de TI	NO EFECTIVO		Contar con un sistema alterno en el cual se apliquen las modificaciones, actualizaciones, parches y verificar que estos no afecten los datos almacenados y el comportamiento en sí el sistema para luego ser aplicado en el sistema que se encuentra en producción.

Existen las declaraciones de aseguramiento de la integridad del software del sistema entregados por los proveedores para todo el software del sistema (incluyendo todas las modificaciones) y considera las exposiciones resultantes en el software del sistema. Los parámetros del software del sistema aseguran que el personal apropiado de TI seleccionó los correctos con el fin de asegurar la integridad de los datos y los programas almacenados en el sistema.				

Cuadro 4.10

Evaluación de pruebas AI3.3

DOMINIO: ADQUISICION E IMPLEMENTACION				
AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica				
AI3.3 Mantenimiento de la Infraestructura				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Existen políticas y procedimientos para el mantenimiento preventivo de hardware para reducir la frecuencia y el impacto de las fallas de desempeño. Se cumple con los pasos y la frecuencia de mantenimiento preventivo prescritos por el proveedor para cada dispositivo de hardware operado por la función de servicios de información y los usuarios afectados se adhieren a ellos. *Probando que:* El calendario de mantenimiento	Entrevista al jefe de TI. Revisión del Contrato de Mantenimiento de Hardware.	EFECTIVO	Contrato de Mantenimiento preventivo y correctivo de equipos de comunicación.	

preventivo de hardware asegura que éste no tendrá un impacto negativo sobre aplicaciones críticas o sensitivas. El mantenimiento programado asegura que no ha sido planeado para periodos pico de carga de trabajo y que la función de servicios de información y las operaciones de los grupos de usuarios afectados son suficientemente flexibles para adaptar el mantenimiento preventivo rutinario planeado. Los programas operativos de servicios de información aseguran que existen las preparaciones adecuadas para manejar anticipadamente los tiempos muertos de hardware ocasionados por mantenimiento no programado.				

Cuadro 4.11

Evaluación de pruebas DS2.3

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS2 Administración de Servicios prestados por terceros				
DS2.3 Administración de Riesgos del Proveedor				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: El contenido de los contratos incluye por lo menos: - Requerimientos de seguridad - Garantías de confidencialidad *Probando que:* El contenido de los contratos incluye por lo menos: - Requerimientos de seguridad - Garantías de confidencialidad La lista de seguridad de acceso incluye únicamente un número mínimo de proveedores requeridos, y que dicho acceso es el mínimo necesario.	Revisión de contratos con proveedores de servicios. Entrevista al jefe de TI.	NO EFECTIVO	Contratos con proveedores de servicios.	Establecer como norma y requerimiento para los proveedores que incluyan aspectos relativos a la seguridad en su propuesta de contratos de servicios.

Cuadro 4.12

Evaluación de pruebas DS4.2

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS4 Garantizar la continuidad del servicio				
DS4.2 Planes de Continuidad de TI				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: La inclusión de los siguientes puntos como contenido mínimo en cada plan de continuidad: - Procedimientos de emergencia para garantizar la seguridad de todos los miembros del personal afectado. *Probando que:* Se han dado el entrenamiento y la concientización de los usuarios y del personal de la función de servicios de información en cuanto a funciones, tareas y responsabilidades específicas dentro del plan.	Revisión de contratos con proveedores de servicios. Entrevista al jefe de TI.	EFECTIVO	Planes de Contingencia existentes.	

Cuadro 4.13

Evaluación de pruebas DS4.3

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS4 Garantizar la continuidad del servicio				
DS4.3 Recursos Críticos de Tecnología de la Información				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: - Una lista de los recursos de sistemas que requieren alternativas (hardware, periféricos, software). - Una lista de las aplicaciones priorizadas de mayor a menor, de los tiempos de recuperación requeridos y de las normas de desempeño esperadas. - La identificación de equipo específico y necesidades de suministros tales como impresoras de alta velocidad, firmas, formatos, equipo de comunicación, teléfonos, etc., así como de una fuente y otras fuentes alternativas definidas.	Aplicación de lista de chequeo al jefe de TI.	NO EFECTIVO		Crear un procedimiento para la identificación de recursos críticos de TI, donde se tomen en cuenta recursos físicos, de software, y de información.

Probando que: El vicerrectorado aprueba la información y operaciones críticas.				

Cuadro 4.14

Evaluación de pruebas DS4.5

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS4 Garantizar la continuidad del servicio				
DS4.5 Pruebas del plan de Continuidad de TI				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: La programación de pruebas, los resultados de la última prueba y las acciones correctivas llevadas a cabo tomando como base la(s) prueba(s) anterior(es). *Probando que:* El plan ha sido probado recientemente y que éste trabajó de acuerdo con lo esperado, o que cualquier deficiencia encontrada trajo como resultado la aplicación de correcciones al plan.	Solicitar informe de resultado de las pruebas del plan de contingencia. Entrevista al jefe de TI.	NO EFECTIVO	Planes de Contingencia existentes.	Actualizar los planes de Contingencia existentes, establecer una programación para realizar pruebas de eficiencia y satisfacción de cada plan elaborado.

Cuadro 4.15

Evaluación de pruebas DS4.8

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS4 Garantizar la continuidad del servicio				
DS4.8 Recuperación y Reanudación de Servicios de TI				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Las alternativas de reanudación del negocio para todos los usuarios estableciendo sitios de trabajo alternativo, una vez que los recursos de sistemas de información estén disponibles (por ejemplo, el sistema ha sido recuperado en el sitio alterno pero el edificio de los usuarios sufrió un incendio y no está disponible). Los planes de contingencia para usuarios son desarrollados tomando como base la no disponibilidad de los recursos físicos para llevar a cabo procesamientos críticos – manuales y computarizados.	Recopilación y revisión de Documentos con procedimientos alternativos para usuarios.	NO EFECTIVO	Planes de Contingencia existentes.	Elaborar documentos con procedimientos de continuación de actividades para usuarios en caso de no disponer de los recursos físicos críticos.

Probando que: Los procedimientos manuales alternativos son documentados y probados como parte de la prueba global.				

Cuadro 4.16

Evaluación de pruebas DS4.9

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS4 Garantizar la continuidad del servicio				
DS4.9 Almacenamiento de respaldo fuera de las instalaciones				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: El detalle de los proveedores de servicios contratados, de los servicios y de las expectativas de respuesta. La información logística de la localización de recursos claves, incluyendo el centro de cómputo de respaldo para la recuperación de sistemas operativos, aplicaciones, archivos de datos, manuales de operación y documentación de programas / sistema / usuarios. Los sistemas de imágenes, los sistemas de fax, los documentos en papel asi como los microfilms y los medios de almacenamiento son parte del plan de continuidad	Entrevista al jefe de TI	NO EFECTIVO	Manual de Procedimientos para realización de respaldos de información.	Definir la contratación de un proveedor para el almacenamiento de respaldos en un sitio alterno diferente a las instalaciones fisicas de la UPS.

Probando que: Las relaciones y tiempos del proveedor contratado son consistentes con las expectativas y necesidades del usuario. El contenido del sitio de respaldo está actualizado y es suficiente con respecto a los procedimientos normales de rotación en el sitio alterno.				

Cuadro 4.17

Evaluación de pruebas DS5.1

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS5 Garantizar la seguridad de los sistemas				
DS5.1 Administración de la Seguridad de TI				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario, como soporte *Probando que:* Los parámetros de seguridad del sistema tienen como base estándares locales/del proveedor.	Solicitar documento de políticas de seguridad. Entrevista al jefe de TI. Revisión del Plan de Contingencia.	NO EFECTIVO	Plan de contingencia	Establecer un plan especifico de seguridad de TI aplicado a los sistemas y los usuarios.

Cuadro 4.18

Evaluación de pruebas DS5.3

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS5 Garantizar la seguridad de los sistemas				
DS5.3 Administración de Identidad				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Se cuenta con perfiles de seguridad de usuario que representen "los menos accesos requeridos" y que muestren revisiones regulares a los perfiles por parte de la administración con fines de reacreditación. Los mecanismos de autenticidad en uso proveen las siguientes facilidades: • uso individual de datos de autenticación • autentificación múltiple • autenticación basada en políticas • Autenticación por demanda	Entrevista al jefe de TI. Correr herramienta que ayude a detectar problemas con claves y vulnerabilidades de seguridad en los servidores de aplicación.	NO EFECTIVO	Reporte remitido por software	Definir nuevas políticas de creación y mantenimiento de contraseña y controlar su cumplimiento.

La politica de contraseña incluye: • Forzar el cambio inicial del mismo la primera vez de uso • longitud adecuada mínima de la clave • la frecuencia obligada minima de cambio de este • verificación de la contraseña en la lista de valores no permitidos • protección adecuada para las claves de emergencia				

Cuadro 4.18 continuación

Evaluación de pruebas DS5.3

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS5 Garantizar la seguridad de los sistemas				
DS5.3 Administración de Identidad				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Los procedimientos de marcación telefónica incluyen: autenticación basada en token o dial-back, cambios frecuentes del número telefónico, firewalls de hardware y software para restringir el acceso a los activos y cambios frecuentes de las claves de acceso y desactivación de las claves de acceso de los empleados temporales *Probando que:* TI cumple con los estándares de seguridad relacionados con: • autenticación y acceso • administración de perfiles de usuario y clasificación de la seguridad de datos		NO EFECTIVO		

Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema				

Cuadro 4.19

Evaluación de pruebas DS5.4

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS5 Garantizar la seguridad de los sistemas				
DS5.4 Administración de cuentas de usuario				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: El número de sesiones concurrentes correspondientes al mismo usuario están limitadas. La política de contraseña incluye: - Forzar el cambio inicial de clave en el primer uso – longitud mínima de contraseña -frecuencia obligada de cambio de la misma. - Verificación de la contraseña en la lista de valores no permitidos (Ej., verificación de diccionario). - Protección adecuada de contraseñas de emergencia. Se cuenta con reportes de fallas a la seguridad y procedimientos formales de	Solicitar documento de políticas de seguridad. Entrevista al jefe de TI.	EFECTIVO	Solicitudes de creación de usuarios en diferentes sistemas. Documentos de entrega de claves para usuarios.	

solución de problemas. Estos reportes deberán incluir: • intentos no autorizados de acceso al sistema • intentos no autorizados de acceso a los recursos del sistema • privilegios de acceso a recursos por ID de usuario • modificaciones autorizadas a las definiciones y reglas de seguridad • accesos autorizados a los recursos • cambio de estatus de la seguridad del sistema *Probando que:* IT cumple con los estándares de seguridad en: - Autenticación de usuarios. - Administración de perfiles de usuario y clasificación de la seguridad de datos. - Existen procedimientos para la requisición, establecimiento y mantenimiento del acceso de usuarios al sistema. - Los contratos de los proveedores de acceso externo incluyen consideraciones sobre responsabilidades y procedimientos de seguridad				

Cuadro 4.20

Evaluación de pruebas DS5.5

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS5 Garantizar la seguridad de los sistemas				
DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Se cuenta con reportes de fallas a la seguridad y procedimientos formales de solución de problemas. Estos reportes deberán incluir: - Intentos no autorizados de acceso al sistema. - Intentos no autorizados de acceso a los recursos del sistema. - Intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad. - Privilegios de acceso a recursos por identificación de usuario. - Modificaciones autorizadas a las definiciones y reglas de seguridad de	Entrevista al jefe de TI. Revisión de manuales de procedimientos.	NO EFECTIVO	Manuales de procedimientos existentes.	Definir un procedimiento y responsable para revisar posibles incidentes de violación de seguridad.

TI. - Accesos autorizados a los recursos (seleccionados por usuario o recurso). - Cambio de estatus de la seguridad del sistema. - Accesos a las tablas de parámetros de seguridad del sistema operativo. *Probando que*: TI cumple con los estándares de seguridad relacionados con: reportes y revisión gerencial de las violaciones e incidentes de seguridad. Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes.				

Cuadro 4.21

Evaluación de pruebas DS5.6

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS5 Garantizar la seguridad de los sistemas				
DS5.6 Definición de Incidente de Seguridad				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Se cuenta con un plan de seguridad estratégico que proporcione una dirección y control centralizados sobre la seguridad de los sistemas de información, así como requerimientos de seguridad de usuario, como soporte. Se utilizan rutas confiables para transmitir información sensitiva. Las medidas de control defectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador.	Entrevista al jefe de TI. Revisión del plan de contingencia.	NO EFECTIVO		Actualizar los planes de contingencia existentes en lo referente al manejo de incidentes de seguridad. Definir un procedimiento para la elaboración de reportes de los incidentes de seguridad.

Probando que: Se emiten reportes de seguridad en cuanto a la oportunidad, precisión y respuesta gerencial a incidentes.				

Cuadro 4.22

Evaluación de pruebas DS5.9

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS5 Garantizar la seguridad de los sistemas				
DS5.9 Prevención, detección y corrección de software malicioso				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: El entrenamiento de los empleados incluye un conocimiento y conciencia sobre seguridad, las responsabilidades de los propietarios y los requerimientos de protección contra virus. Las medidas de control detectivo y preventivo han sido establecidas por la administración para prevenir y detectar virus de computador. *Probando que:* Los procedimientos para la protección contra software	Revisión de manuales de manejo y uso de los recursos de TI para los empleados. Entrevista al jefe de TI.	EFECTIVO	Documento de Políticas de TI.	

malicioso incluyen: □ Todo el software adquirido por la organización se revisa contra los virus antes de su instalación y uso. □ Existe una política por escrito sobre descargue de archivos, aceptación y uso de software, freeware y shareware y esta política está vigente. - El software para aplicaciones altamente sensibles está protegido por MAC (Código de Autentificación de Mensajes) o firma digital, y se utilizan mecanismos, fallas de verificación para evitar el uso del mismo inapropiadamente.				

Cuadro 4.22 continuación

Evaluación de pruebas DS5.9

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS5 Garantizar la seguridad de los sistemas				
DS5.9 Prevención, detección y corrección de software malicioso				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
- Los usuarios tienen instrucciones para la detección y reportes de virus, como el desempeño lento o crecimiento misterioso de archivos. - Existe una política y un procedimiento vigente para la verificación de disquetes obtenidos por fuera del programa de compra normal de la organización.		EFECTIVO		

Cuadro 4.23

Evaluación de pruebas DS5.10

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS5 Garantizar la seguridad de los sistemas				
DS5.10 Seguridad de la Red				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: El hardware y software de seguridad, así como los módulos criptográficos, están protegidos contra la intromisión o divulgación, el acceso se limita a la base de la "necesidad de conocer". Las medidas de control preventivo y de detección han sido establecidas por la administración para prevenir y detectar virus de computador. *Probando que:* Los firewalls poseen por lo menos las siguientes propiedades	Aplicar una herramienta para detectar las vulnerabilidades de la red. Identificar la existencia de un Firewall y sus reglas definidas actualmente. Entrevista al jefe de T.I.	EFECTIVO	Configuración de reglas de firewall, IPS	

- Todo el tráfico de adentro hacia fuera y viceversa debe pasar por estos firewalls (esto no debe limitarse a los controles lógicos, debe reforzarse físicamente). - Sólo se permitirá el paso al tráfico autorizado, como se define en la política de seguridad local. - Los firewalls por sí mismo es inmune a la penetración. - El tráfico de intercambio en el firewall se lleva a cabo en la capa de aplicación únicamente.				

Cuadro 4.23 Continuación

Evaluación de pruebas DS5.10

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS5 Garantizar la seguridad de los sistemas				
DS5.10 Seguridad de la Red				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
- La arquitectura del firewall combina las medidas de control tanto a nivel de la red como de la aplicación. - La arquitectura del firewall provee una auditoria de todas las comunicaciones hacia o a través del sistema del firewall y activara alarmas cuando se detecte alguna actividad sospechosa. - La arquitectura del firewall refuerza la discontinuidad de un protocolo en la capa de transporte. - La arquitectura del firewall debe estar configurada de acuerdo a la "filosofía de arte mínimo". - La arquitectura del firewall debe desplegar sólida autenticación para la administración y sus componentes.		EFECTIVO		

- La arquitectura del firewall oculta la estructura de la red interna. - El host de la organización, que provee el soporte para las solicitudes de entrada al servicio e las redes públicas, permanece fuera del firewall. - La arquitectura del firewall se defiende de los ataques directos (ej. A través del monitoreo activo de la tecnología de reconocimiento de patrones y tráfico). - Todo código ejecutable se explora en busca de códigos maliciosos (ej. virus, aplicaciones dañinas) antes de introducirse.				

Cuadro 4.24

Evaluación de pruebas DS5.11

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS5 Garantizar la seguridad de los sistemas				
DS5.11 Intercambio de Datos Sensitivos				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Existen módulos criptográficos y procedimientos de mantenimiento de llaves, si éstos son administrados centralizadamente y si son utilizados para todas las actividades de acceso externo y de transmisión. El acceso a los datos de seguridad así como la administración de la seguridad, datos de transacciones sensitivas, claves y llaves criptográficas se limita a la base de la "necesidad de conocer". Se utilizan rutas confiables para transmitir información sensitiva no encriptada.	Recopilar información sobre las transacciones sensitivas que se realicen. Entrevista al jefe de TI.	EFECTIVO		

Probando que: T.I. cumple con los estándares de seguridad relacionados con: - Autenticación y acceso - Estándares de administración de llaves criptográficas Existen llaves secretas para la transmisión.				

Cuadro 4.25

Evaluación de pruebas DS9.3

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS9 Administración de los configuración				
DS 9.3 Revisión de Integridad de la Configuración				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Existen procedimientos de control de cambios de software para: - Establecer y mantener una librería de programas de aplicación con licencia. - Asegurar que la librería de programas de aplicación con licencia sea controlada adecuadamente. - Asegurar la confiabilidad e integridad del inventario de software. - Asegurar la confiabilidad e integridad del inventario de software autorizado utilizado y revisar la existencia de software no autorizado.	Revisión de manuales de manejo y uso de los recursos de TI para los empleados. Solicita el inventario de software instalado en las Computadoras personales. Solicitar el inventario de licencias	NO EFECTIVO	Documento de Políticas de TI. Inventarios de Software y de licencias de programas instalados.	Establecer un procedimiento de control de software no autorizado e incluir en las políticas de seguridad y manejo de los recursos de TI. Este procedimiento debe darse a conocer a los empleados oportunamente. Hacer seguimiento sobre el

- Asignar responsabilidades sobre el control de software no autorizado a un miembro específico del personal. - Registrar el uso de software no autorizado y reportar a la administración para llevar a cabo acciones correctivas. - Determinar si la administración llevó a cabo acciones correctivas sobre las violaciones.				cumplimiento de este procedimiento.

Cuadro 4.25 continuación

Evaluación de pruebas DS9.3

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS9 Administración de los configuración				
DS 9.3 Revisión de Integridad de la Configuración				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Probando que: Para todas las computadoras personales que contengan software no autorizado se reporten violaciones y la administración lleve acciones correctivas. Existen mecanismos para asegurar que no existan software no autorizado en las computadoras, incluyendo: - Políticas y normas/estatutos. - Entrenamiento y conciencia de responsabilidades potenciales. - Formas firmadas de cumplimiento por parte de todo el personal que utiliza computadoras.		NO EFECTIVO		

- Control centralizado del software computacional. - Revisión continúa del software computacional. - Reportes de los resultados de la revisión. - Acciones correctivas por parte de la administración, basadas en los resultados de las revisiones.				

Cuadro 4.26

Evaluación de pruebas DS11.7

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS11 Administración de datos				
DS 11.7 Chequeos de exactitud, suficiencia y autorización				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Para la entrada de datos: - Los documentos fuente siguen un proceso de aprobación apropiada antes de su captura. - Existe una separación de funciones apropiada entre las actividades de envío, aprobación, autorización y entrada de datos. - Existen pistas de auditoría para identificar la fuente de entrada. - Existen rutinas de verificación para la edición de los datos capturados tan cerca del punto de origen como sea posible. - Existen procesos apropiados de	Entrevista al jefe de TI. Solicitar manuales de procedimientos para el procesamiento de datos.	NO EFECTIVO		Establecer políticas y procedimientos para el manejo de integridad y autenticación de la información, así como para el manejo de errores en los datos.

manejo de datos de entrada erróneos. *Probando que:* La entrada de datos: El envío a proceso de datos de prueba (tanto transacciones correctas como erróneas) para asegurar que se llevan a cabo revisiones de precisión, suficiencia y autorización. Para transacciones seleccionadas se comparan los archivos maestros antes y después de la captura.				

Cuadro 4.27

Evaluación de pruebas DS11.8

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS11 Administración de datos				
DS 11.8 Manejo de Errores en la Entrada de Datos				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Para el procesamiento de datos: Los programas contienen rutinas de prevención, detección y corrección de errores: - los programas deben probar las entradas en cuanto a errores (por ejemplo, validación y edición) - los programas deben validar todas las transacciones contra una lista maestra los programas deben rechazar la anulación de condiciones de error. Los procesos de manejo de errores incluyen:	Entrevista al jefe de TI. Solicitar manuales de procedimientos para el procesamiento de datos.	NO EFECTIVO		Establecer procedimientos escritos para la corrección y renvío de datos con errores.

La corrección de errores y renvío de la transacción debe ser aprobado. Existen procedimientos por escrito para la corrección y renvío de datos con errores incluyendo una solución que no afecte su reprocesamiento. Las transacciones renviadas son procesadas exactamente como fueron procesadas originalmente. La responsabilidad de la corrección de errores reside dentro de la función de envío original.				

Cuadro 4.27 continuación

Evaluación de pruebas DS11.8

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS11 Administración de datos				
DS 11.8 Manejo de Errores en la Entrada de Datos				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Probando que: El procesamiento de datos: Se envían datos de prueba (tanto transacciones correctas como erróneas) para asegurar que se llevan a cabo la validación, autenticación y edición de procesamiento de datos tan cerca del punto de origen como sea posible. El proceso de manejo de errores es llevado a cabo de acuerdo con los procedimientos y controles establecidos. Se llevan a cabo la retención,		NO EFECTIVO		

solución y revisión apropiada de la integridad en el manejo de errores y que éstas funcionan adecuadamente. Los procedimientos y acciones del manejo de errores cumplen con los procedimientos y controles establecidos.				

Cuadro 4.28

Evaluación de pruebas DS11.9

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS11 Administración de datos				
DS 11.9 Integridad de procesamiento de datos				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Para el procesamiento de datos: Los programas contienen rutinas de prevención, detección y corrección de errores: - Los programas deben probar las entradas en cuanto a errores (por ejemplo, validación y edición). - Los programas deben validar todas las transacciones contra una lista maestra. - Los programas deben rechazar la anulación de condiciones de error. Los procesos de manejo de errores incluyen:	Entrevista al jefe de TI Solicitar manuales de procedimientos para el procesamiento de datos.	NO EFECTIVO		Establecer procedimientos escritos para la corrección y renvío de datos con errores. Establecer responsables para el control y cumplimiento de los procedimientos y políticas propuestos.

- La corrección de errores y renvío de la transacción debe ser aprobado. - Existen bitácoras de los programas ejecutados y las transacciones procesadas/rechazadas para pistas de auditoría. - Las tablas utilizadas en la validación son revisadas frecuentemente.				

Cuadro 4.28 continuación

Evaluación de pruebas DS11.9

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS11 Administración de datos				
DS 11.9 Integridad de procesamiento de datos				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
- Existe un grupo de control para monitorear las actividades de entrada e investigar los eventos no estándar, así como balancear las cuentas de registros y totales de control para todos los datos procesados. - Existen procedimientos por escrito para la corrección y renvio de datos con errores incluyendo una solución que no afecte su reprocesamiento. - Las transacciones renviadas son procesadas exactamente como fueron procesadas originalmente. - La responsabilidad de la corrección de errores reside dentro de la función de envio original. *Probando que:*		NO EFECTIVO		

El procesamiento de datos: - Se utilizan efectivamente los totales de control paso a paso y los controles de actualización de archivos maestros.				

Cuadro 4.29

Evaluación de pruebas DS11.10

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS11 Administración de datos				
DS 11.10 Validación y Edición de procesamiento de Datos				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Para el procesamiento de datos: Los programas contienen rutinas de prevención, detección y corrección de errores: - Los programas deben probar las entradas en cuanto a errores (por ejemplo, validación y edición). Los procesos de manejo de errores incluyen: Los sistemas de Inteligencia Artificial están colocados en un marco referencial de control interactivo con operadores humanos para aseguran	Entrevista al jefe de T. I.	EFECTIVO	Listado de preguntas aplicado al jefe de T.I. Ver Anexo	

que las decisiones importantes se aprueben. *Probando que:* El procesamiento de datos: Se envían datos de prueba (tanto transacciones correctas como erróneas) para asegurar que se llevan a cabo la validación, autenticación y edición de procesamiento de datos tan cerca del punto de origen como sea posible.				

Cuadro 4.30

Evaluación de pruebas DS11.23

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS11 Administración de datos				
DS 11.23 Respaldos y Restauraciones				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Existen estrategias de respaldo y restauración de medios. Los respaldos de medios se llevan a cabo de acuerdo con la estrategia de respaldos y si la utilidad de los respaldos es verificada regularmente. Los respaldos de medios son almacenados con seguridad y si las localidades de almacenamiento son revisadas periódicamente en cuanto a la seguridad de sus acceso físico y a la seguridad de los archivos de datos y otros elementos. *Probando que:*	Entrevista al jefe de T. I. Aplicación de listado de preguntas al jefe de TI.	EFECTIVO	Manuales y procedimientos para la realización de respaldos. Listado de preguntas aplicado al jefe de T.I. Ver Anexo	

Confirmar la creación e integridad de los respaldos en asociación con el procesamiento normal, así como para los requerimientos del plan de continuidad.				

Cuadro 4.31

Evaluación de pruebas DS11.24

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS11 Administración de datos				
DS 11.24 Funciones de Respaldo				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Los respaldos de medios se llevan a cabo de acuerdo con la estrategia de respaldos y si la utilidad de los respaldos es verificada regularmente. *Probando que:* Revisar los procedimientos de creación de respaldos para asegurar la existencia de datos suficientes en caso de desastre.	Entrevista al jefe de T. I. Aplicación de listado de preguntas al jefe de TI.	EFECTIVO	Manuales y procedimientos para la realización de respaldos. Listado de preguntas aplicado al jefe de T.I. Ver Anexo	

Cuadro 4.32

Evaluación de pruebas DS11.27

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS11 Administración de datos				
DS 11.27 Protección de mensajes sensitivos				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Para las salidas, interfaces y distribución: Existen pistas de auditoria para facilitar el seguimiento del procesamiento de transacciones y la reconciliación de datos alterados. Existe una definición clara sobre aspectos de seguridad durante las salidas, interfaces y distribución. Las fallas en seguridad durante cualquier fase son comunicadas a la administración, se llevan a cabo acciones correctivas sobre ellas y son reflejadas apropiadamente en nuevos procedimientos.	Entrevista al jefe de T. I. Solicitar manuales de procedimientos para el procesamiento de datos	EFECTIVO	Listado de preguntas aplicado al jefe de T.I. Ver Anexo	

Para la autenticación e integridad de información: La integridad de los archivos de datos se verifica periódicamente. La firma electrónica o la certificación se utilizan para verificar la integridad y autenticidad de los documentos electrónicos entrantes.				

Cuadro 4.32 continuación

Evaluación de pruebas DS11.27

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS11 Administración de datos				
DS 11.27 Protección de mensajes sensitivos				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Probando que: La Salida, Interface y Distribución de Datos: Las pistas de auditoría son proporcionadas para facilitar el seguimiento del procesamiento de transacciones en la reconciliación de datos confusos o erróneos. Los reportes de salida son revisados en cuanto a su precisión por parte del proveedor y los usuarios relevantes. Existen la retención, solución y revisión apropiada de la integridad en el manejo de errores y que éstas funcionan adecuadamente. Existe una protección adecuada de		EFECTIVO		

información sensitiva durante la transmisión y transporte en cuanto a accesos y modificaciones no autorizadas. Para la integridad y autenticación de la información: Existen protecciones adecuadas para asegurar la integridad, confidencialidad y no rechazo de los mensajes sensitivos transmitidos sobre Internet o cualquier otra red pública.				

Cuadro 4.33

Evaluación de pruebas DS11.29

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS11 Administración de datos				
DS 11.29 Integridad de transacciones electrónicas				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Para las salidas, interfaces y distribución: Existen pistas de auditoría para facilitar el seguimiento del procesamiento de transacciones y la reconciliación de datos alterados. Existe una definición clara sobre aspectos de seguridad durante las salidas, interfaces y distribución. Las fallas en seguridad durante cualquier fase son comunicadas a la administración, se llevan a cabo acciones correctivas sobre ellas y son reflejadas apropiadamente en nuevos procedimientos.	Entrevista al jefe de TI. Entrevista a los usuarios de las aplicaciones que implican transacciones electrónicas.	EFECTIVO		

Para la autenticación e integridad de información: La integridad de los archivos de datos se verifica periódicamente. La firma electrónica o la certificación se utilizan para verificar la integridad y autenticidad de los documentos electrónicos entrantes.				

Cuadro 4.33 continuación

Evaluación de pruebas DS11.29

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS11 Administración de datos				
DS 11.29 Integridad de transacciones electrónicas				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Probando que: La Salida, Interface y Distribución de Datos: Existen la retención, solución y revisión apropiada de la integridad en el manejo de errores y que éstas funcionan adecuadamente. Los procedimientos y acciones de manejo de errores cumplen con las políticas y controles establecidos. Existe la protección adecuada para la información sensible durante la transmisión y transporte contra los accesos no autorizados y las modificaciones.		EFECTIVO		

Para la integridad y autenticación de la información: Existen protecciones adecuadas para asegurar la integridad, confidencialidad y no rechazo de los mensajes sensitivos transmitidos sobre Internet o cualquier otra red pública.				

Cuadro 4.34

Evaluación de pruebas DS12.2

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS12 Administración del Ambiente Físico				
DS 12.2 Medidas de Seguridad Física				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: La localización de las instalaciones no es obvia externamente, se encuentra en el área u organización menos accesible, y si el acceso es limitado al menor número de personas. Los procedimientos de acceso lógico y físico son suficientes, incluyendo perfiles de seguridad de acceso para empleados, proveedores, equipo y personal de mantenimiento de las instalaciones.	Entrevista al jefe de TI. Revisión del listado sobre seguridad física de TI. Observaciones en el sitio	EFECTIVO	Listado de preguntas aplicado al jefe de T.I. Ver Anexo	

administración de llave y lectora de tarjetas son adecuados, incluyendo la actualización y revisión continua tomando como base una "menor necesidad de acceso". Las políticas de acceso y autorización de entrada/salida, escolta, registro, pases temporales requeridos, cámaras de vigilancia son apropiadas para todas las áreas y especialmente para las áreas más sensibles. Las medidas de control de seguridad y acceso incluyen a los dispositivos de información portátiles utilizados fuera del sitio.				

Cuadro 4.34 continuación

Evaluación de pruebas DS12.2

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS12 Administración del Ambiente Físico				
DS 12.2 Medidas de Seguridad Física				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Se lleva a cabo una revisión de los registros de visitantes, asignación de pases, escolta, persona responsable del visitante, bitácora para asegurar tanto los registros de entradas como de salidas y el conocimiento de la recepcionista con respecto a los procedimientos de seguridad. Existe una revisión del proceso de alarma al ocurrir una violación a la seguridad, que incluya: - Definición de la prioridad de la alarma (por ejemplo, apertura de la puerta por parte de una persona armada que ha entrado en las		EFECTIVO		

instalaciones). - Escenarios de respuesta para cada alarma de prioridad. - Responsabilidades del personal interno versus personal de seguridad local o proveedores. - Interacción con las autoridades locales. - Revisión del simulacro de alarma más reciente. La organización es responsable del acceso físico dentro de la función de servicios de información, incluyendo: - Desarrollo, mantenimiento y revisiones continuas de políticas y procedimientos de seguridad.				

Cuadro 4.34 continuación

Evaluación de pruebas DS12.2

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS12 Administración del Ambiente Físico				
DS 12.2 Medidas de Seguridad Física				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
- Establecimiento de relaciones con proveedores relacionados con la seguridad. - Contacto con la administración de las instalaciones en cuanto a problemas de tecnología relacionados con seguridad. - Coordinación del entrenamiento y conciencia sobre seguridad para la organización. - Coordinación de actividades que afecten en control de acceso lógico vía aplicaciones centralizadas y software de sistema operativo. - Proporcionar entrenamiento y crear conciencia de seguridad no sólo dentro de la función de servicios de		EFECTIVO		

información, sino para los servicios de usuarios. *Probando que:* Los armarios cableados están físicamente protegidos con el acceso posible autorizado y el cableado se encuentra bajo tierra o conductos protegidos tanto como sea posible. La bitácora de visitantes sigue apropiadamente los procedimientos de seguridad. Existen los procedimientos de identificación requeridos para cualquier acceso dentro o fuera vía observación.				

Cuadro 4.34 continuación

Evaluación de pruebas DS12.2

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS12 Administración del Ambiente Físico				
DS 12.2 Medidas de Seguridad Física				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Las puertas, ventanas, elevadores, ventilas y ductos o cualquier otro modo de acceso están identificados. El sitio computacional está separado, cerrado y asegurado y es accesado únicamente por personal de operaciones y gente de mantenimiento tomando como base un "acceso necesario". Los planes físicos son actualizados a medida que cambian la configuración, el ambiente y las instalaciones. No se almacenan útiles peligrosos.		EFECTIVO		

Existe el seguimiento de auditoría de control de acceso sobre software de seguridad o reportes clave de administración. Se llevan a cabo verificaciones de suficiencia de administración clave de acceso. Se otorga una educación en seguridad física y conciencia de seguridad. Existe una cobertura y experiencia de seguros para los gastos asociados con algún evento de seguridad, pérdida del negocio y gastos para recuperar la instalación.				

Cuadro 4.35

Evaluación de pruebas DS12.4

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS12 Administración del Ambiente Físico				
DS 12.4 Protección contra factores ambientales				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Se lleva a cabo una revisión de los procedimientos de aviso contra incendio, cambios de clima, problemas eléctricos y procedimientos de alarma, así como las respuestas esperadas en los distintos escenarios para los diferentes niveles de emergencias ambientales. Se lleva a cabo una revisión de los procedimientos de control de aire acondicionado, ventilación, humedad y las respuestas esperadas en los distintos escenarios de pérdida o extremos no anticipados.	Entrevista al jefe de TI. Revisión del listado sobre seguridad física de TI. Observaciones en el sitio	EFECTIVO	Listado de preguntas aplicado al jefe de T.I. Ver Anexo	

Probando que: Los planes físicos son actualizados a medida que cambian la configuración, el ambiente y las instalaciones. Los registros y el equipo de monitoreo ambiental y de seguridad -- debajo, en, sobre, y alrededor – son mantenidos. No se almacenan útiles peligrosos.				

Cuadro 4.36

Evaluación de pruebas DS12.5

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE				
DS12 Administración del Ambiente Físico				
DS 12.5 Administración de Instalaciones Físicas				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Existen elementos de infraestructura especificos alternativos necesarios para implementar seguridad: - Fuente de poder ininterrumpida UPS *Probando que:* Prueba de UPS y verificar que los resultados cumplan con los requerimientos operacionales de capacidad para sostener las actividades criticas de procesamientos de datos.	Entrevista al jefe de TI. Solicitud de documentación técnica de equipos UPS.	EFECTIVO	Documentos relacionados con la adquisición de unidades de UPS.	

Cuadro 4.37

Evaluación de pruebas ME3.1

DOMINIO: MONITOREO Y EVALUACION				
ME3 Garantizar el cumplimiento con requerimientos externos				
ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Evaluación de controles: Si los procedimientos de seguridad van de acuerdo con los requerimientos legales y si estos están tomados en cuenta adecuadamente, incluyendo: - protección con "passwords" o contraseñas y software para limitar el acceso - procedimientos de autorización - medidas de seguridad de terminales - medidas de encriptación de datos - controles de Firewalls - protección contra virus - seguimiento de reportes de violaciones	Se solicita manual de procedimientos. Se entrevista al jefe de TI.	NO EFECTIVO		Elaborar procedimientos de seguridad para el área de TI, donde se contemple medidas de encriptación de datos, controles de Firewalls y otros. Establecer un procedimiento para el Comercio Electrónico que cumpla con los requerimientos legales y políticas de la empresa; y

Existen políticas y procedimientos para: - Asegurar las acciones correctivas apropiadas relacionadas con la revisión oportuna de los requerimientos externos y si existen procedimientos para asegurar un cumplimiento continuo. - Coordinar la revisión de los requerimientos externos, con el fin de asegurar que se aplican oportunamente las acciones correctivas que garantizan el cumplimiento de los requerimientos externos. - Proporcionar la dirección/enfoque adecuados sobre privacidad de tal manera que todos los requerimientos legales caigan dentro de este alcance. .				que éste sea también cumplido por el proveedor de servicio contratado

Cuadro 4.37 continuación

Evaluación de pruebas M3.1

DOMINIO: MONITOREO				
ME3 Garantizar el cumplimiento con requerimientos externos				
ME3.1 Identificar los Requerimientos de las Leyes, Regulaciones y Cumplimientos Contractuales				
REVISION A TRAVES DE:	**DESCRIPCION DE LA PRUEBA**	**EVALUACION**	**DOCUMENTOS DE SOPORTE**	**RECOMENDACION**
Probando que: En donde se hayan impuesto límites regulatorios a la encriptación que pueda ser utilizada (Ej. Longitud de la llave), la encriptación aplicada cumpla con las regulaciones. En donde las regulaciones o procedimientos internos requieran la protección y/o encriptación especial de ciertos elementos de datos (Ej. número de identificación personal, claves de acceso), dicha protección/encriptación sea proporcionada a estos datos.	Se solicita manual de procedimientos. Se entrevista al jefe de TI.	NO EFECTIVO		Elaborar procedimientos de seguridad para el área de TI, donde se contemple medidas de encriptación de datos, controles de Firewalls y otros. Establecer un procedimiento para el Comercio Electrónico que cumpla con los requerimientos legales y políticas de la empresa; y

Los datos transmitidos a través de las fronteras internacionales no violan las leyes de exportación. Los contratos existentes con los proveedores de comercio electrónico consideren adecuadamente los requerimientos especificados en las políticas y procedimientos organizacionales.				que éste sea también cumplido por el proveedor de servicio contratado

ANÁLISIS DE RESULTADOS

En base a la evaluación de las pruebas efectuadas sobre la gestión de la seguridad en redes se determinó que el 50% de los objetivos de control detallados cumplen con las condiciones necesarias para su efectivo cumplimiento. A continuación se detalla el funcionamiento actual de estos controles:[7]

PO4.10 Segregación de funciones

Actualmente, existen los documentos que especifican las funciones a realizarse por el personal del Departamento y su nivel de responsabilidad en cada una de ellas, esto es, manejado por el jefe de T.I. Sin embargo en la entrevista realizada al mismo recalca que por el límite de personal del Departamento, casi todas las funciones son conocidas por el personal, y en la mayoria de funciones están en capacidad de realizar casi todas las tareas si es necesario.

PO6.11 Comunicación para educar y concienciar sobre seguridad de TI.

El Documento de Políticas de T.I. es proporcionado por la sede cuenca, sin embargo puede ser modificado para adaptarse a las necesidades locales, el mismo es dado a conocer a todos los colaboradores que ingresan a laborar en el departamento, y se les requiere su firma de aceptación sobre las posibles acciones a tomar si éste no es cumplido a cabalidad en cuanto al manejo de la información de los recursos de T.I.

AI3.2 Mantenimiento preventivo para hardware

El contrato para el servicio de mantenimiento de hardware, en su contenido, define las visitas periódicas anuales para realizar el mantenimiento preventivo tanto de computadores, como de impresoras y terminales; los calendarios son definidos anticipadamente conforme se acerca la terminación de un período, tomando en cuenta que no se realicen en fines de mes, para las áreas de Contabilidad y Recursos Humanos, aunque eso solo se cumple en los dos primeros años de adquirir un producto, luego de eso el propio personal de T.I se encarga de esa función especifica teniendo una persona responsable de toda la operación.

DS4.3 Contenido del Plan de Continuidad de TI

Los Planes de Contingencia existentes, contienen los puntos necesarios para garantizar la continuidad del servicio en caso de presentarse un evento o falla del sistema que impida su funcionamiento normal. Cuenta principalmente con procedimientos de emergencia, medios de comunicación con responsables dentro y fuera de la universidad, que intervienen en la recuperación del servicio y métodos de funcionamiento manual para continuar con el servicio.

DS5.3 Seguridad de Acceso a Datos en Líneas

Los principales sistemas de la universidad, cuentan con usuarios y claves de acceso para su ingreso, previo la creación de cada usuario se define por parte del departamento correspondiente tanto el nivel de usuario y perfil con el que debe ser creado, de este modo se limita el acceso al manejo de datos dentro de los sistemas. Se puede también hacer revisión de registros de actividades de usuario en el sistema ya sea de ingreso de notas, contable o el directorio activo.

DS5.4 Administración de cuentas de usuario

Existe una definición de perfiles de usuario para el ingreso a los sistemas, están establecidas políticas para cambio de contraseñas, y se cuenta con solicitudes formales para la creación de usuarios y acceso a sistemas que deben ser presentadas a la jefatura de T.I. Cuando colaboradores dejan de trabajar para el departamento, Recursos Humanos informa a Sistemas sobre la separación de colaborador para deshabilitar el usuario respectivo.

DS5.9 Administración de Derechos de Acceso e Identificación Centralizada

Esta definida la política de creación de usuarios de forma que el jefe de un Área debe presentar el formato de solicitud de creación y el perfil acorde a éste.
Una vez creado el usuario y clave, éste se da a conocer al mismo jefe por medios escritos y de igual manera se informa de la creación de un

usuario en un sistema determinado al departamento de Recursos Humanos.

DS5.16 Sendero Seguro

Falta de transacciones de datos sensitivos fuera de la organización, la única transacción posible es la que se da por acreditación de sueldos en la cuenta de cada empleado a través de la página web de la entidad bancaria que presta el servicio y que garantiza la seguridad adecuada para realizar este tipo de transacciones.

DS5.19 Prevención, detección y corrección de software malicioso

En el documento de políticas de TI existe recomendaciones para los usuarios sobre el uso de los recursos de TI sobre todo de acciones preventivas para evitar los virus y troyanos, mientras que la responsabilidad de las acciones correctivas esta a cargo del personal de TI.

DS5.20 Arquitectura de Firewalls y conexión a redes públicas

La organización cuenta con una aplicación proxy que se encuentra en los servidores centrales, así como un IPS marca Cisco y que está configurada para ejercer los controles de seguridad para la organización, en cuanto a lo que tiene que ver con puertos habilitados, transferencia de archivos via e-mail, posibles ataques de virus, spams, intrusiones a la red, tuneles etc.

DS11.10 Validación y Edición de procesamiento de Datos

La validación de datos esta manejada y controlada en cada uno de los sistemas que se manejan en la empresa.

DS11.23 Respaldos y Restauraciones y DS11.24 Funciones de Respaldo

Existen procedimientos para la realización de respaldos y restauraciones de la información. La localización física para el almacenamiento de los respaldos dentro del área de Sistemas, son

adecuados para su mantención, sin embargo no existe un lugar de almacenamiento externo de la información respaldada.

DS11.27 Protección de Mensajes Sensitivos y DS11.29 Integridad de transacciones electrónicas

La única transacción electrónica que se realiza con terceros y a través del Internet es la acreditación de los sueldos de los empleados en cada una de sus cuentas bancarias y la integridad de esta transacción esta controlada directamente por procedimientos del banco.

DS12.1 Seguridad Física

En base a las observaciones realizadas se determinó que el Área de Sistemas cuenta con todo la seguridad fisica necesaria para la protección de servidores y equipos de comunicación. Así como un control adecuado de acceso que ha ido mejorando con el paso del tiempo.

DS12.5 Protección contra factores ambientales

La UPS cuenta con un equipamiento adecuado para detección y control de incendio, humedad, cambio de temperatura y ventilación en el Área de Servidores y equipos de comunicación.

DS12.6 Suministro ininterrumpido de energía

Recientemente fue reparada una unidad de UPS para soportar los equipos de computación de todo el lugar. Algunas de ellas están destinadas únicamente a soportar la carga del Departamento de Sistemas, esto es servidores equipos de telecomunicaciones y computadores, la otra unidad cubre la carga del resto de Departamentos, a excepción de Contabilidad y el área de Negocios, que tienen otro sistema de UPS. La carga que soporta cada unidad de UPS actualmente es de aproximadamente un 30%, por lo que uno de ellos puede soportar la carga del otro en caso de presentarse una emergencia. Cabe anotar que equipos de impresión láser, copiadoras y máquinas de fax no cuentan con este sistema de UPS.

M3.7 Competencia de la función de aseguramiento independiente

Se cuenta con una empresa aseguradora que cumple con todos los requerimientos y objetivos de la empresa; cuya solidez en el servicio ha sido probada y garantizada.

4.2 Informe final de la auditoria

Los informes preliminar y final que se presentan a continuación, tuvieron su discusión y análisis previo con el responsable del área de T.I. dentro de la organización, en este caso el jefe de T.I.[12]

INFORME PRELIMINAR DE LA AUDITORÍA Y SU DISCUSIÓN

Alcance de la Auditoría

- Conocer los aspectos fundamentales que intervienen en la gestión de seguridad en la red de datos.
- Determinar y valorar las fortalezas y debilidades de la gestión de la seguridad actual en la red de datos de la Universidad Politécnica Salesiana
- Proponer mejoras que permitan minimizar o eliminar los problemas actuales en la gestión de seguridad en la red de datos.
- Evaluar algunas de las mejoras propuestas mediante el estudio de casos factibles de desarrollo.

Objetivos de la Auditoría

- Analizar y diagnosticar la actual gestión de seguridad en la red de datos del departamento de Ti de la UPS.
- Plantear las mejoras para la gestión de la seguridad de la red de datos.
- Proponer nuevos procesos y actividades que ayudarán a identificar los controles que se requieren para garantizar la seguridad de la información.

Temas Considerados Críticos

Análisis de Riesgos

Observación:

No existen procedimientos para la identificación de los recursos tecnológicos críticos y la administración de los posibles riesgos. Los planes de contingencia existentes no están actualizados y no están acorde con la situación actual de los recursos tecnológicos identificados.

Recomendaciones:

- Establecer procedimientos para identificar los recursos criticos de la empresa, riesgos potenciales y la incidencia que estos producirían en el cumplimiento de los objetivos de la empresa.
- Elaborar planes de contingencia para cada uno de los recursos críticos identificados.
- Actualizar los planes de contingencia existentes.

Resultado de la discusión con el jefe de TI:

El jefe de TI manifiesta que los últimos planes de contingencia y pruebas de los mismos se los realizó por motivo del año 2007, cuando se paso todo los equipos del centro de datos de la localidad anterior a la nueva sede y que no se han presentado cambios significativos en los recursos críticos de TI ni los planes de contingencia que se aplican a estos.

Aseguramiento del Servicio Continuo

Observación:

No se cuenta con un sitio alterno con toda la tecnología necesaria para la reanudación de la actividad del negocio en caso de haber un desastre. No se tiene un sitio alterno para el almacenamiento de los respaldos de datos críticos de la universidad, aunque se ha cambiado aquello ya que parcialmente ciertos datos se almacenas en paralelo en el centro de datos de la UPS sede cuenca.

Recomendaciones:

- Establecer procedimientos para determinar un sitio alterno que cuente con todos los equipos y sistema de comunicación necesario para la continuidad de los procesos y elaborar planes de contingencia que contengan toda la información necesaria para la recuperación y funcionamiento de todos los sistemas en el nuevo sitio. También será necesario establecer un lugar alterno donde guardar los respaldos de la información de los sistemas críticos.
- Es importante que se realicen pruebas del plan de contingencia para determinar su correcto funcionamiento y se evalúen los tiempos de ejecución de cada actividad para que se dé una respuesta rápida.

Resultado de la discusión con el jefe de TI:

La naturaleza del negocio no hace necesario contemplar un sitio alterno con los equipos necesarios para *garantizar* la continuidad del negocio, además esto implicaria un gasto que no se justifica.
Sobre el sitio alterno para el almacenamiento de respaldos no se ha podido concretar por falta de apoyo del Departamento Financiero local y de la sede cuenca para contratar este servicio, pero el requerimiento esta hecho y se espera su cumplimiento a un corto plazo.

Garantizar la seguridad de sistemas

Observación:

Falta de reportes de fallas de seguridad ni procedimientos formales para dar solución a problemas.
Falta de cláusulas específicas en los contratos con terceros para garantizar la confidencialidad de los datos de la empresa.
Existe una política muy general para la prevención de uso de software no autorizado.

Recomendaciones:

- Es necesario establecer procedimientos y responsables del registro y seguimiento de las fallas de seguridad así como de sus soluciones.
- Exigir que en los contratos con terceros se especifique todo lo referente a la confidencialidad de los datos de la universidad.

- Mejorar la política existente sobre el uso de software no autorizado, dar a conocer al empleado y realizar evaluaciones periódicas al empleado para asegurarse de su cumplimiento.

Resultado de la discusión con el jefe de TI:

Los reportes de las fallas y problemas no son considerados relevantes ya que se considera que las personas que conforman el Departamento de Sistemas conocen las soluciones de los mismos.
La parte legal en lo que se refiere a los contratos de servicios con terceros se la encarga a los abogados de la entidad.
Aunque las políticas sobre el uso de software no permitido no esta perfectamente definidas, la forma de prevenir esta situación es la negación de permisos a los usuarios.

Administración de Datos

Observación:

Falta de procedimientos para el chequeo, exactitud, suficiencia y autorización de los datos que se ingresan, solamente se da un respaldo físico para almacenaje.
En los sistemas principales existe rutinas para el manejo de errores e integridad de datos, sin embargo no existen procedimientos documentados para la corrección y renvío de datos críticos.

Recomendaciones:

- Establecer procedimientos que garanticen el ingreso correcto de los datos sobre todo aquellos ingresados en forma manual.
- En el caso de datos erróneos se deberá definir un procedimiento formal para su rectificación.

Resultado de la discusión con el jefe de TI:

Se considera que los procedimientos de los sistemas son suficientes para garantizar el correcto manejo y procesamiento de los datos y no es prioridad tener una documentación al respecto.

INFORME FINAL DE LA AUDITORÍA

Informe Final de Auditoria

UPS, Guayaquil

Febrero de 2012

Señores

UPS, Cuenca

Atte. Jefe de T.I.

De nuestra consideración:

Me dirijo a Ud. a efectos de poner a consideración el trabajo de Auditoria aplicada a la Gestión de Seguridad de la Red de Datos usando como metodología COBIT (Control Objetives Information Technologies) practicada desde Junio a Noviembre del 2011, y en base al análisis y procedimientos aplicados a las informaciones recopiladas se emite el presente informe.

Fecha de Inicio de la Auditoria: Junio del 2011
Fecha de Redacción del Informe de la Auditoria: Febrero del 2012
Auditor:
José Patino S.

Alcance de la Auditoria

- Conocer los aspectos fundamentales que intervienen en la gestión de seguridad en la red de datos.
- Determinar y valorar las fortalezas y debilidades de la gestión de la seguridad actual en la red de datos de la UPS sede Guayaquil
- Proponer mejoras que permitan minimizar o eliminar los problemas actuales en la gestión de seguridad en la red de datos.
- Evaluar algunas de las mejoras propuestas mediante el estudio de casos factibles de desarrollo.

Objetivos de la Auditoria

- Analizar y diagnosticar la actual gestión de seguridad en la red de datos de la universidad,
- Plantear las mejoras para la gestión de la seguridad de la red de datos.
- Proponer nuevos procesos y actividades que ayudarán a identificar los controles que se requieren para garantizar la seguridad de la información.

Objetivos de Control Considerados Críticos

PO2.3 Esquema de Clasificación de Datos

Observación:

No se cuenta con procedimientos de clasificación de datos, ni responsables de datos sensitivos, no hay registros de datos borrados o compartidos y sus respectivas autorizaciones para estas actividades.

Riesgo:

Acceso a datos no definidos acorde a su criticidad, los datos que no están bien clasificados no tienen un adecuado plan de recuperación. La política de TI no contempla la reclasificación de la información por su sensibilidad.

Recomendaciones:

Crear un procedimiento para la clasificación de datos con el responsable de los mismos, según la criticidad e importancia.

PO9.3 Identificación de Eventos

Observación:

Falta de procedimiento específico para la identificación de riesgos de TI, solamente se maneja una evaluación de los riesgos en base al criterio de los empleados del Área de TI según los objetivos del negocio.

Riesgo:

Al no identificarse los riesgos de TI no se consideran las posibles amenazas, vulnerabilidades, y consecuencias a las que esta expuesto el negocio, por lo tanto no es posible medir el impacto y pérdidas económicas de un ataque o falla de un recurso crítico.

Recomendación:

Definir procedimientos para identificar los recursos criticos y riesgos potenciales sobre éstos. Asegurarse del cumplimiento de los mismos y verificar que estén acorde con los objetivos del negocio.

PO9.5 Respuesta a los Riesgos

Observación:

Al no estar identificados los riesgos de TI no es posible establecer un Plan de Acción contra Riesgos que mitigue los problemas causados por una amenaza.

Riesgo:

De presentarse un ataque o falla sobre un recurso crítico no se cuenta con acciones establecidas para recuperarse y garantizar el servicio continuo del negocio, esto puede llevar a producir pérdidas económicas y de prestigio de la entidad.

Recomendación:

Conjuntamente con la identificación de los riesgos potenciales debe definirse la creación de planes de acción contra posibles riesgos, los responsables de llevarlos a cabo y la asignación de los recursos necesarios sean estos de carácter humano o financiero para la ejecución de este plan.
Debe tomarse en cuenta que estos planes han de ser revisados y probados periódicamente para asegurar su funcionamiento y efectividad.

DS5.1 Administración de la Seguridad de TI

Observación:

La organización no cuenta con un plan definido de seguridad de T.I., los planes de contingencia existentes tampoco contemplan posibles ataques a la seguridad del sistema.

Riesgo:

De no existir un plan de seguridad, no se establecen medidas de seguridad para la prevención de ataques o fallas de seguridad, tampoco se definen acciones a tomar para la recuperación de una de estas amenazas y no es posible cuantificar el impacto en el normal desarrollo de las actividades del negocio.

Recomendación:

Centralizar la administración de la seguridad de la información de manera que estén acordes con los objetivos del negocio.
Definir responsabilidades para la elaboración, actualización, ejecución y monitoreo del plan de seguridad.

DS5.2 Administración de Identidad

Observación:

El acceso a los recursos de T.I. está limitado al personal que cuenta con un usuario y contraseña claramente definido, pero no existe un control estricto sobre el manejo de cuentas, en lo que tiene que ver con sesiones múltiples de un mismo usuario; los cambios de clave no son obligatorios para todos los sistemas, únicamente para el directorio activo, para el acceso a servidores los nombres de usuario y claves no pueden ser cambiados por los usuarios, sino únicamente por el Departamento de T.I. con solicitud formal para el cambio.

Riesgo:

Posible divulgación de claves de usuario, con exposición a uso no adecuado o malintencionado de éstas, lo que ocasiona no poder identificar responsabilidades en la manipulación de datos.

Recomendación:

Establecer nuevas políticas y procedimientos para la administración de cuentas de usuarios y contraseñas, tanto en servidores como aplicaciones, que contemple cambios de password inicial, cambios periódicos de clave y limitación del número de conexiones con el mismo usuario.

DS5.4 Administración de Cuentas de Usuario

Observación:

Los derechos de acceso a recursos, asignados a las cuentas, no son sujetos a revisiones después de su creación, ya que el perfil que se le asigna es establecido por el jefe de Área en cuestión.

En cuanto a aplicaciones especificas, como educativo, y RRHH el sistema lleva un registro de accesos de usuario que es revisado únicamente cuando se sospecha de una violación en la seguridad o mal ingreso de datos.

Riesgo:

Al no contar con logs en todos los sistemas no se puede identificar responsabilidades en caso de accesos no autorizados o mal intencionados a los recursos y perfiles de usuario mal asignados.

Recomendaciones:

Creación de archivos logs para las aplicaciones que registren el acceso de las cuentas y los recursos que utilizan. Revisión periódica de los registros existentes.

DS5.4 Administración de Cuentas de Usuario (Continuación)

Observación:

El Sistema de directorio activo es el único que cuenta con notificaciones para el usuario sobre el cambio de clave periódica, el resto de aplicaciones no cuentan con este servicio y en el caso de los servidores las cuentas tienen deshabilitada la opción de cambio periódico. En cuanto al registro de número de intentos de acceso o la fecha de último ingreso no se registra ni en los servidores ni en las aplicaciones.

Riesgo:

La falta de control de los accesos a recursos por parte de los mismos usuarios provocaría mal uso de las cuentas y desconocimiento de posibles problemas que puedan presentarse en el funcionamiento de la misma.

Recomendaciones:
Implementar notificaciones tanto para el cambio de clave como para el límite de intentos para acceso y sesiones múltiples con la misma cuenta. Una vez implementado este procedimiento instruir a los usuarios al respecto.

DS5.5 Pruebas, Vigilancia y Monitoreo de Seguridad

Observación:

No se realizan notificación sobre violaciones de seguridad ni se toman acciones para prevenir, detectar o superar la incidencia provocada, salvo el caso de reportar desperfectos en hardware o software.

Riesgo:

No se determinan responsables directos o indirectos de un incidente de seguridad. No se determina fecha, origen y hora del incidente de seguridad. No se toman acciones inmediatas para superar el incidente de seguridad ni para prevenir incidencias futuras.

Recomendaciones:

Definir procedimientos y responsabilidades para la revisión de registros e identificación de posibles violaciones de seguridad existentes y buscar soluciones que las superen o minimicen, sea esto implementación de nuevas reglas de firewall, ips parches o actualizaciones de los sistemas.

PO6.4 Implantación de Políticas de TI

Observación:

Los usuarios tienen conocimiento del documento de políticas de TI pero no se realizan evaluaciones para verificar la comprensión y el cumplimiento de las políticas.

Riesgo:

Se puede caer en el mal uso de los recursos y datos de la empresa. Fuga de la información crítica de la empresa. Los procedimientos de uso de los recursos no se realizan según los estándares y poner en riesgo la seguridad de los datos.

Recomendaciones:

Evaluar periódicamente a los usuarios sobre el entendimiento de las políticas del uso de TI.

4.3 Ejecución y evaluación de algunos de los procesos propuestos.

A continuación se preponen varios procesos para obtener una mejora en el control de la seguridad, sin embargo es necesario aclarar que COBIT no ofrece soluciones a los posibles problemas encontrados dentro del área informática, por lo que los procesos que se proponen a continuación son una contribución adicional basados en los resultados obtenidos para mejorar el control existente en la organización.

Se consideraron los procesos propuestos y evaluados para los siguientes Objetivos de Control:

CUADRO 4.38

EJECUCION Y EVALUACIÓN PROCESOS PROPUESTOS

DOMINIO: ENTREGA DE SERVICIO Y SOPORTE		
PO6 Comunicación de los objetivos y aspiraciones de la Gerencia		
PO6.4 Implementación de Políticas de TI.		
RECOMENDACIÓN	**PROCESO PROPUESTO**	**EVALUACION**
Establecer procedimientos de evaluación a usuarios, en cuanto a lo que tiene que ver con el cumplimiento de políticas de seguridad, y otros procedimientos relativos a controles.	- Se creará un documento con normas del manejo de seguridad de datos para los empleados que se les da a conocer al ser contratados. Este documento controlará la seguridad de los datos que manipulan los usuarios y los niveles de responsabilidad sobre los mismos según el cargo que tengan. - Se harán evaluaciones a los usuarios sobre el conocimiento de la seguridad en la manipulación de los datos.	- Este documento cumple con su objetivo al ser conscientemente seguido por los usuarios. - Según la evaluación aplicada el 60% de los empleados manejan responsablemente los datos. Tanto los datos del trabajo diario (documentos de Word, Excel, e-mail etc.) como los de los sistemas

CUADRO 4.38 continuación

EJECUCION Y EVALUACIÓN PROCESOS PROPUESTOS

DOMINIO: ADQUISICION E IMPLEMENTACION		
AI3 Adquisición y Mantenimiento de la Infraestructura Tecnológica		
AI3.2 Protección y Disponibilidad del Recurso de infraestructura		
RECOMENDACIÓN	**PROCESO PROPUESTO**	**EVALUACION**
Contar con un sistema alterno en el cual se apliquen las modificaciones, actualizaciones, parches y verificar que estos no afecten los datos almacenados y el comportamiento en sí del sistema para luego ser aplicado en el sistema que se encuentra en producción.	- El jefe de Sistemas se encargará de asignar un equipo alterno donde se instalen los sistemas que demanden actualizaciones o modificaciones frecuentes para ser probadas antes de ser instaladas en los sistemas que están en producción. - En estos sistemas de pruebas se harán revisiones frecuentes de los datos que manejen obteniendo muestras mediante reportes y verificando si están correctos una vez que se haya hecho una actualización o aplicado un parche.	- La aplicación de parches y actualizaciones en el equipo alterno ha ayudado a prevenir problemas en el sistema que esta en producción y los datos no se han visto afectados. Aunque mantener un equipo alterno implica mantenerlo gran tiempo ocioso porque las actualizaciones no son tan frecuentes.

CUADRO 4.38 continuación

EJECUCION Y EVALUACIÓN PROCESOS PROPUESTOS

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE		
DS2 Administración de Servicios prestados por Terceros		
DS2.3 Administración de Riesgos del Proveedor		
RECOMENDACIÓN	**PROCESO PROPUESTO**	**EVALUACION**
Establecer como norma y requerimiento para los proveedores que incluyan aspectos relativos a la seguridad en su propuesta de contratos de servicios.	- En el caso de requerir servicio de terceros referentes a TI se exigirá al Área de Sistemas agregar cláusulas dentro de los contratos que contemplen garantizar la confidencialidad e integridad de los datos según sea el tipo de servicio que se esté contratando sobre todo cuando haya transmisiones de datos criticos mediante la red así como la información que se les facilite a personas de otras empresas que estén prestando servicios dentro de las instalaciones del hotel.	- Se ha propuesto cláusulas adicionales para ser agregadas, referentes a la seguridad de datos en lo contrato con el proveedor de Internet, así como con el de Mantenimiento de Equipos.

CUADRO 4.38 continuación

EJECUCION Y EVALUACIÓN PROCESOS PROPUESTOS

DOMINIO: ENTREGA DE SERVICIOS Y SOPORTE		
DS4 Aseguramiento del servicio continuo		
DS4.5 Pruebas del Plan de continuidad de TI		
RECOMENDACIÓN	**PROCESO PROPUESTO**	**EVALUACION**
Actualizar los planes de Contingencia existentes, establecer una programación para realizar pruebas de eficiencia y satisfacción de cada plan elaborado.	- Se establecerá una persona encargada de revisar los planes de contingencia existentes y realizar las actualizaciones necesarias tomando en cuenta las áreas críticas que se han detectado. - Los Planes de contingencia serán probados dos veces al año para revisar su correcto funcionamiento y en caso de haber fallar deberán ser corregidos. - El plan de contingencia deberá contemplar también determinar un lugar estratégico y contratar todos los servicios de tecnología y comunicación necesarios desde donde funcionará los sistemas principales para la actividad de la empresa.	- Se elaboró un nuevo plan de contingencia que se tomará como base para ser actualizado anualmente. - Este plan se está poniendo a consideración de la jefatura para su aprobación y asignación de recursos. - Una vez aprobado el plan se procederá a las respectivas pruebas.

BIBLIOGRAFÍA

1. ARCERT – SUSSECRETARIA DE TI. "Manual de Seguridad en Redes", Argentina., 2000
2. JOSE PATIÑO SANCHEZ – IVONNE MARTIN. "Desarrollo de Políticas de Seguridad Informática e Implementación de cuatro dominios en base a la Norma 27002 para el Área de Hardware en la empresa Uniplex Systems S.A. en Guayaquil" Ecuador, (Tesis de la Facultad de Ingeniería en Sistemas de La Escuela Superior Politécnica del Litoral)., Junio 2009.
3. CONTRERAS – OCHOA – SOLIS. "Introducción a la seguridad en internet y aplicaciones" versión 1.0.0., 2004
4. ANTONIO VILLALON HUERTA. "Seguridad en unix y redes", versión 2.1., Julio 2002
5. Comité Directivo de COBIT y IT Governance Institute, "*Alineando CobiT® 4.1, ITIL® V3 y ISO/IEC 27002 en beneficio de la empresa" USA, versión 2.7., 2008*
6. ICONTEC, Norma Técnica Colombiana, Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información, Edición Noviembre 16 del 2007., Referencia NTC-ISO/IEC 27002.
7. Comité Directivo de COBIT y IT Governance Institute, "*COBIT Resumen Ejecutivo" USA, versión 4.1., 2007*
8. Comité Directivo de COBIT y IT Governance Institute, "*COBIT Objetivos de Control" USA, versión 4.1., 2007*
9. Comité Directivo de COBIT y IT Governance Institute, "*COBIT Marco Referencial" USA, versión 4.1., 2007*
10. Comité Directivo de COBIT y IT Governance Institute, "*COBIT Directrices Gerenciales" USA, versión 4.1., 2007*
11. Comité Directivo de COBIT y IT Governance Institute, "*COBIT Herramientas de implementación" USA, versión 4.1., 2007*
12. Comité Directivo de COBIT y IT Governance Institute, "*Directrices de Auditoria" USA, Segunda Edicion., 2000*
13. ISO – IEC., Estándar Internacional ISO/IEC 17799. Tecnología de la Información – Técnicas de Seguridad – Código para la práctica de Seguridad de la Información., Segunda Edición. Junio 15 del 2005.
14. UNIVERSIDAD POLITECNICA SALESIANA, "Propuesta de Estructura Orgánica Funcional y de Responsabilidades para las Áreas de Información" versión 1.0., Enero 2011
15. Comité Directivo de COBIT y IT Governance Institute, "COBIT Marco Referencial" USA, versión 5.0., 2012
16. WEBSIDE, información obtenida de los siguientes vínculos de Red:

http://www.ongei.gob.pe/publica/metodologias/Lib5007/21.HTM
http://sgsi-iso27001.blogspot.com/
http://iso.org
http://isaca.org

CONCLUSIONES

- COBIT está diseñado para ofrecer a la alta dirección una visión general de la situación actual de la tecnología de información, para conocer sus mayores debilidades y fortalezas; y de cómo éstas pueden afectar al cumplimiento de los objetivos gerenciales, más no puede ser considerado como una respuesta netamente tecnológica y de información para el área de informática de la empresa.

- El estudio y conocimiento de los documentos COBIT es necesario para lograr un enfoque adecuado de la auditoria y por ende resultados reales y que ayuden al cumplimiento de los objetivos de la facultad.

- COBIT no proporciona una estructura formal ni especifica cómo desarrollar un plan de auditoria y su ejecución posterior, en su lugar, ofrece una serie de guías de cómo realizar el análisis y evaluación de los controles existentes en la empresa en el área de tecnología de la información y que están relacionados con el alcance de los objetivos de la empresa.

- COBIT enfoca sus documentos y guías para la auditoria en los Procesos COBIT, por esto, no siempre este enfoque coincide exactamente con el área informática que se desea auditar, de aquí que se hizo necesario realizar un trabajo de investigación y de documentación adicional por parte del auditor para lograr la concatenación con los Objetivos COBIT relacionados y el área a auditar.

- De la discusión del informe preliminar de la auditoria se concluye que no existe una conciencia más formal por parte de la jefatura de T.I. para asegurar la correcta gestión de la seguridad.

- El no tener identificados correctamente los recursos críticos de T.I. puede acarrear el no contar con planes de continuidad adecuados y por lo tanto propensos a sufrir un ataque de seguridad, pérdida de información, etc. De los cuales será casi imposible recuperarse sin causar pérdidas económicas a la organización.

- Por ultimo es necesario definir los responsables de cada recurso de la organización y de su protección, siendo conveniente delimitar claramente el área de responsabilidad de cada persona para que no existan huecos ni problemas de definiciones claras de responsabilidades.

RECOMENDACIONES

- Documentar los procedimientos operativos, cualquiera que sea su tipo, detallándose para cada tarea sus requerimientos de programación, interdependencias con otros sistemas, tareas de mantenimiento previstas y procedimientos de recuperación ante incidentes.

- Realizar análisis periódicos de los riesgos y monitorear continuamente la situación, pues la seguridad que se requiere proporcionar con unas políticas de gestión de la seguridad es permanente para lo cual es necesario de un proceso continuo, más no de acciones puntuales

- Definir procedimientos específicos para el establecimiento de controles efectivos dentro de la gestión de seguridad, como la implementación de revisiones de posibles violaciones a la seguridad y accesos no autorizados.

- Establecer conjuntamente con la participación del vicerrectorado el nivel de participación y de importancia del área tecnológica dentro de la universidad, no sólo tomando en cuenta el papel que se cumple dentro del cumplimiento de las labores de los demás colaboradores, sino también considerando su grado crítico en lo referente al servicio brindado a los estudiantes no solo en cuanto a navegación y otros servicios de Internet, sino en cuanto al nivel de seguridad que se le debe ofrecer para la realización de sus actividades estudiantiles.

- Los Planes de Contingencia actuales no cumplen con los niveles necesarios de información, se debe establecer un nuevo procedimiento para su creación, definición y realización de pruebas de funcionamiento, etc.

- Mejorar el procedimiento de gestión de cuentas y contraseñas para estar acorde a los estándares de seguridad y políticas de password.

- La seguridad de la información debe ser considerada como un proceso de mejoramiento continuo y no un estado estático, en donde los nuevos requerimientos de seguridad se ajusten a los cambios de la empresa.

- Realizar una redistribución de funciones que defina la responsabilidad de realizar una correcta gestión de seguridad de la red, y en caso de ser necesario contemplar la posible contratación de una persona adicional para ayudar a mejorar la gestión de la seguridad en la organización.

- Se recomienda a COBIT como una herramienta para realizar el análisis y evaluación de los puntos críticos de la organización, tomando como base las

Directrices de Auditoría, documento bastante específico en donde se detallan todas evaluaciones a los controles existentes.

- Si bien COBIT brinda en sus documentos las herramientas necesarias para el proceso de auditoría, es conveniente tener un conocimiento básico de cómo desarrollar una auditoría informática y de esta manera explotar mejor todas las bondades de COBIT.

Anexo 1

POSIBLE IMPLEMENTACIÓN DEL PROYECTO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA INTRANET DE LA FACULTAD DE SISTEMAS DE LA UPS

A) Manual de Procedimientos para la Implementación del PGSI

A continuación se describe una parte del manual de procedimientos para implementar el PGSI en la facultad de sistemas de la UPS.

Política de Seguridad de la Información

Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo. Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades del Organismo y de los titulares de Unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

Objetivo

Proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política. Mantener la Política de Seguridad de la empresa actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Establecer las directrices, los procedimientos y los requisitos para asegurar la protección oportuna y correcta de los equipos computacionales de la UPS sede Guayaquil y el uso adecuado de los mismos.

Alcance

Esta Política se aplica en todo el ámbito del Organismo, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

La finalidad de las políticas de seguridad que se describen en este Anexo, es proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los computadores de la empresa, (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas disciplinarias. Para el desarrollo de las políticas, es necesario considerar las diferentes fuentes de información, que permiten el desempeño diario de las funciones de la corporación. Entre los puntos principales que se deben analizar son: Políticas de seguridad para computadores, comunicaciones

En el cual se debe establecer las directrices, los procedimientos y los requisitos para asegurar la protección oportuna y correcta de los equipos computacionales y sistemas de comunicaciones de la entidad y el uso adecuado de los mismos.

Políticas de seguridad para redes

El propósito de este manual es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la empresa al estar conectada a redes de computadoras.

En el desarrollo de estas políticas se debe definir los términos, condiciones y limitantes del servicio de Correo Electrónico Interno y limitantes del servicio de Internet corporativo de la empresa.

ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

Generalidades

Es necesario tener bien definido un marco de gestión para efectuar diferentes tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades, para tener una eficiente administración de la seguridad de información.

Debe tenerse en cuenta que ciertas actividades de la empresa pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Objetivo

- Administrar la seguridad de la información dentro de la Corporación y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.
- Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

En este control es necesario definir un Comité de Seguridad que entre sus funciones deberá:

- Revisar y proponer a la máxima autoridad de la empresa para su aprobación, la Política y las funciones generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro del Organismo.
- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información del Organismo frente a interrupciones imprevistas.

Una vez integrado el Comité, es necesario se definan las funciones de los miembros del mismo para poder para que este pueda desempeñar sus actividades y mejorar la seguridad en la empresa. En la implementación están especificados los miembros del Comité.

El Comité de Seguridad de la Información debe proponer al vicerrectorado local y luego a la sede cuenca para su aprobación la definición y asignación de las responsabilidades que surjan de sus funciones.

Es necesario definir el proceso para la autorización de nuevos recursos para el procesamiento de información así como los requerimientos de Seguridad en contratos con Terceros, los principales puntos que se deben considerar lo siguiente:

a) Cumplimiento de la Política de seguridad de la información de la UPS.

b) Protección de los activos de la Corporación, incluyendo:

- Procedimientos para proteger los bienes de la Corporación, abarcando los activos físicos, la información y el software.
- Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
- Restricciones a la copia y divulgación de información.

c) Descripción de los servicios disponibles.

d) Nivel de servicio esperado y niveles de servicio aceptables.

e) Permiso para la transferencia de personal cuando sea necesario.

f) Obligaciones de las partes del acuerdo y responsabilidades legales.

g) Definiciones relacionadas con la protección de datos.

h) Acuerdos de control de accesos que contemplen:

- Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
- Proceso de autorización de accesos y privilegios de usuarios.
- Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

i) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.

j) Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.

k) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

l) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

m) Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.

n) Proceso claro y detallado de administración de cambios.

o) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

p) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.

q) Controles que garanticen la protección contra software malicioso.

r) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

Gestión de los Activos de Red

Generalidades

La Corporación debe tener conocimiento sobre los activos que posee como parte importante de la administración de riesgos.

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección. Clasificar la información para señalar su sensibilidad y criticidad.

Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Responsabilidad sobre los activos

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada.

El Responsable de sistemas es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la Política.

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de 4 meses. El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

En la implementación del manual, se especifica el inventario realizado así como los responsables de cada activo. Una vez realizado el inventario, se debe clasificar el activo, en base a tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad, los cuales se revisaron al inicio de este capítulo. Para clasificar la información se consideró una de las siguientes categorías:

CRITICIDAD BAJA: ninguno de los valores asignados supera el 2.

CRITICIDAD MEDIA: alguno de los valores asignados es 2

CRITICIDAD ALTA: alguno de los valores asignados es 3

Sólo el propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos: cambios necesarios para que los usuarios conozcan la nueva clasificación.

SEGURIDAD DE LOS RECURSOS HUMANOS

Generalidades

La seguridad de la información se basa en la capacidad para conservar la integridad, confidencialidad y disponibilidad de los activos.

Para lograr lo anterior es fundamental educar e informar al personal desde su ingreso y en forma continua, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad. Así mismo, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

Objetivo

Reducir los riesgos de error humano, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Indicar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Corporación en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información. Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Seguridad en la definición del trabajo y los recursos

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

En la implementación se especifica el procedimiento para la proceso de selección del personal.

Términos y condiciones de la relación laboral

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede de la empresa y del horario normal de trabajo.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de contrato.

Conocimiento, educación y entrenamiento de la seguridad de información

Todos los empleados de la empresa y, cuando sea necesario, los usuarios externos y los terceros que desempeñen funciones en la empresa, deberán recibir una adecuada capacitación y actualización periódica en materia de la política de seguridad, normas y procedimientos para la seguridad. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la Política.

Cada 6 meses se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

El personal que ingrese a la Corporación recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Además se otorgará una guía de usuario para que tengan un mejor conocimiento con respecto a las amenazas informáticas y sus posibles consecuencias dentro de la Corporación de tal manera que se llegue a concienciar y crear una cultura de seguridad de la información.

Seguridad Física y del Entorno

Generalidades

La seguridad física y ambiental minimiza los riesgos de daños e interferencias a la información y a las operaciones de la Corporación. Además, trata de evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Organismo.

Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo.

Previo a la implementación de un control de seguridad física y del entorno, es necesario que se realice un levantamiento de información de la situación actual de la Corporación en cuanto a su seguridad física para determinar las vulnerabilidades y posibles soluciones.

En puntos previos de este capítulo ya se realizó la recolección de la información necesaria. En esta parte se define la implementación de los controles de seguridad física y del entorno.

Gestión de Comunicaciones y Operaciones

Generalidades

Debido a los peligros existentes como software malicioso, virus, troyanos, etc. es importante que se adopten controles para prevenir cualquier tipo de amenazas.

Se debe separar los ambientes de pruebas y de operaciones, establecer procedimientos que garanticen la calidad de los procesos operativos para evitar incidentes producidos por la mala manipulación de información.

Las comunicaciones establecidas permiten el intercambio de información, se deberá establecer controles para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones. Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas.

El administrador de la red debe revisar con el encargado legal de la UPS, todos los contratos y acuerdos con terceros, pues es necesario garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Generalidades

Es necesario establecer controles que impidan el acceso no autorizado a los sistemas de información por parte de personal diferente a los que tienen permisos, para lo cual es necesario se implementen procedimientos para controlar la asignación de privilegios de acceso a los diferentes sistemas y aplicativos de la empresa. En estos procedimientos se especifican sugerencias para mejorar el control actual de los accesos de los usuarios a diferentes niveles.

Es importante para la seguridad de la información controlar el acceso a los recursos, y protegerlos contra el acceso no autorizado, modificación o robo.

Para el caso de la UPS se definirán políticas para el control de acceso así como los procedimientos que deben seguirse para poder implementarlos en los sistemas operativos y aplicativos. En los procedimientos considerados se debe tener en cuenta que los mismos consideren identificación, autenticación y autorización de los usuarios.

Objetivo

Entre los principales puntos que se desean cubrir con este control se tienen:

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar de mejor forma la seguridad en conexiones entre UPS y los proveedores externos.
- Mantener un registro de eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Alcance

En el procedimiento para implementar este control, se define una política de control de acceso que se aplica a todos los usuarios internos y externos que tienen diferentes permisos para acceder a los sistemas de información, red de la facultad de sistemas de la UPS sede Guayaquil, bases de datos.

Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

Política de Control de Acceso

- Negar el acceso a sistemas de cuentas anónimas o usuarios no identificados
- Limitar o monitorear el uso de cuentas con privilegios especiales
- Suspender o retardar el acceso a sistemas, aplicaciones después de un número de intentos fallidos.
- Remover cuentas obsoletas de usuarios que han dejado la compañía
- Suspender cuentas inactivas después de 30 o 60 días.

- Reforzar un criterio estricto de acceso
- Deshabilitar las configuraciones por defecto, servicios y puertos no requeridos.
- Reemplazar las configuraciones de contraseñas por defecto en las cuentas
- Limitar y monitorear reglas de accesos globales
- Forzar rotación de la contraseña

- Forzar requerimientos de contraseñas
- Sistemas de auditorias y eventos de usuarios y acciones, así como revisión de reportes periódicos.

Si bien el método biométrico es una forma segura de autentificación e identificación, para el caso de la empresa no aplica pues los sistemas a los cuales acceden y son de mayor riesgo es el aplicativo, al cual ingresan los proveedores que se encuentran fuera de la empresa y no resulta cómodo para los usuarios este tipo de metodología además de resultar más costoso.

Contraseñas

El usuario puede generar su contraseña, pero el sistema operativo fuerza al usuario a que el mismo cumpla con ciertos requerimientos, como por ejemplo que contenga un cierto número de caracteres, que incluya caracteres especiales, que no se relaciones con el nombre del usuario de la máquina.

Además de mantener un registro de las últimas claves ingresadas, la fecha en la que debe cambiarse.

Si una contraseña trata de ser vulnerada también puede configurarse el registro de intentos fallidos de acceso al sistema con lo cual se puede bloquear el acceso al mismo para de esta manera disminuir el riesgo debido a la vulneración de las contraseñas.

Uso de Contraseñas

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.

b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

c) Seleccionar contraseñas de calidad, de acuerdo a las políticas de seguridad establecidas, en las que básicamente tratan los siguientes puntos:

1. Sean fáciles de recordar.

2. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.

3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

e) Cambiar las contraseñas provisorias en el primer inicio de sesión (•log on").

f) Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

Identificación y Autenticación de los usuarios

Todos los usuarios de la empresa deben tener un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En los casos que se requiere compartir un ID de usuario, tanto el administrador de la red como el responsable de cada área debe autorizar dicha compartición, así como definir el tiempo en el cual se requiere que se comparta el ID, luego del cual se debe eliminar el identificador y los privilegios del mismo.

Restricción del acceso a la información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación acorde al procedimiento de asignación de privilegios.

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación, para lo cual el administrador de la red debe manejar los privilegios de acuerdo al perfil del usuario y con los requerimientos realizados formalmente por el responsable de cada área.

b) Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.

c) Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.

d) Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.

e) Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.

f) Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

Protección de los puertos de diagnóstico remoto

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, por lo cual lo primero que debemos determinar es el diagnóstico de que puertos se encuentran abiertos en la red.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Generalidades

En este control se deben revisar las aplicaciones como puntos críticos de vulnerabilidades, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

Con este control se pretende cubrir varios puntos de seguridad, entre los principales objetivos se tienen:

- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
- Definir los métodos de protección de la información crítica o sensible.

Alcance

Los controles que se detallan a continuación se aplican a los sistemas informáticos, y a los sistemas operativos que integran los ambientes por el organismo de donde residen los mismos.

Para implementar un mayor control a la información confidencial o importante de los diferentes departamentos de la empresa.

Se debe entender como información confidencial a toda información que se refiere a planes de negocio, tecnología no anunciada, información financiera no pública, e información personal como son tarjetas de crédito, contraseñas.

La empresa debe tener aprobado un procedimiento de cambios aprobado por la gerencia, y los cambios deben ser documentados y comunicados a los empleados involucrados. En la implementación se especifica el proceso para llevar a cabo un cambio.

Revisión técnica de los cambios en el sistema operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, el administrador de la red debe tener un procedimiento en el cual se incluye:

a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.

b) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación. Para lo cual el administrador debe planificar el día en el cual se llevará a cabo el cambio e informarlo a los usuarios y coordinar con los responsables de cada área en caso de que ellos deban realizar algún trabajo por el cual no pueden suspender sus actividades. Estos cambios deben programarse para fines de semana donde no haya impacto en los usuarios.

c) Asegurar la actualización del Plan de Continuidad de las Actividades del Organismo.

Restricción del cambio de paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del Responsable del Área Informática, se deberá:

a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.

b) Determinar la conveniencia de que la modificación sea efectuada por Uniplex, por el proveedor o por un tercero.

c) Evaluar el impacto que se produce si la empresa se hace cargo del mantenimiento.

d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.

Este es un punto que debe ser analizado con todos los responsables de las áreas y el administrador de la red, deben realmente aprobar los cambios que implica varios procedimientos como son en el ámbito legal, financiero, recursos, etc.

Canales encubiertos y código

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos. El código malicioso está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario.

Para lo cual es necesario que la corporación cuente con un software adecuado instalado en cada máquina de los empleados para evitar problemas debido a canales encubiertos y código troyano.

Además de las medidas implementadas con el antivirus, es necesario que previo la instalación de algún software en la UPS se deba considerar:

a) Adquirir programas a proveedores acreditados o productos ya evaluados.

b) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.

c) Controlar el acceso y las modificaciones al código instalado.

d) Utilizar herramientas para la protección contra la infección del software con código malicioso, en este caso la empresa utilizó el antivirus Eset Nod 32.

Gestión de Incidentes de la Seguridad de la Información

Divulgación de eventos y de debilidades de la seguridad de la información

Es importante que la empresa tenga un procedimiento a seguir cuando se presente un incidente de seguridad en la red, pues es necesario que pueda aprender de los errores y evitar que un ataque ocurra. Por lo cual es importante que luego de cada incidente siga un procedimiento, técnicas, configuraciones necesarias para reforzar lo modificado y mejorar la seguridad.

Es necesario que se tenga un mejor control del uso apropiado de los recursos de la red, en otros términos, todos los recursos de la informática deben usarse de una manera ética y responsable. El uso de recursos de tecnología de información puede categorizarse ampliamente como aceptable, tolerable, o prohibió:

- El uso aceptable de recursos de tecnología de información es el uso legal consistente con los requerimientos de la organización, en base a las políticas de la misma que permitan solventar los problemas de la Corporación.

- El uso tolerable es el uso legal para otros propósitos que no chocan con en la política del uso aceptable de la organización.
- El uso prohibido es el uso ilegal y todo el otro uso que son "aceptables" ni tolerables.

Administración de incidentes y mejoras de la seguridad de la información

Después que el incidente ha sido resuelto, es necesario realizar una documentación del mismo para poder determinar las experiencias aprendidas del mismo. Como resultado de un análisis posterior al reporte de incidentes, el personal de seguridad puede necesitar emitir alarmas o advertencias a todos los empleados de la empresa sobre las acciones tomar para reducir vulnerabilidades que se explotaron durante el incidente.

Entre estas alertas es importante que se especifique de forma clara:

- Asegurar que sólo personal autorizado tiene el acceso a los archivos electrónicos.
- Minimizar el riesgo de modificación desautorizado de archivos electrónicos guardando los datos sensibles en los medios de comunicación trasladables.
- Asegurar que personal apropiado se entrena para proteger los archivos electrónicos sensibles o clasificados
- Proveer del respaldo y recuperación de archivos para proteger contra la pérdida de información
- Asegurar que la seguridad de los archivos electrónicos esté incluido en los planes de seguridad de información globales de su organización.

Gestión de Continuidad del Negocio

Generalidades

Un punto importante para toda organización, es administrar de forma ordenada las actividades necesarias para la continuidad del negocio, en este procedimiento se deben involucrar a todos los empleados de la empresa.

El plan de continuidad debe mantenerse actualizado y ser una parte integrada en los diversos procesos de los diferentes departamentos de la empresa.

Objetivo

Este control es importante para cubrir los puntos críticos de la entidad en caso de algún desastre, a continuación se detallan los principales objetivos:

- Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
- Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:

a) Detección y determinación del daño y la activación del plan.

b) Restauración temporal de las operaciones y recuperación del daño producido al sistema original.

c) Restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

- Asignar funciones para cada actividad definida.

Alcance

Estos controles se aplican a las partes críticas de la entidad.

Aspectos de la gestión de continuidad del negocio

Al desarrollar el plan de la continuidad del negocio para la empresa, se debe considerar los parámetros sobre los cuales se va a desarrollar el mismo para poder los desastres. Para este caso cuando se realizó en análisis de riesgos y vulnerabilidades se consideraron diferentes tipos de desastres como son:

Desastres naturales:

- Inundaciones
- Terremotos
- Fuego
- Derrumbamientos, avalanchas, y otros movimientos de la tierra

Desastres artificiales, es decir aquellos relacionados con la computación:

- Sabotaje de los sistemas informáticos, y de la información
- Ataques terroristas
- Huelgas
- Protestas
- Ataque de Negación de Servicio en los servidores de la red
- Virus, gusanos, y otros ataques informáticos

Y finalmente se debe considerar un tercer grupo:

- Faltas de la infraestructura (interrupciones para uso general, interrupciones de la energía, etc.)
- Fallas de comunicaciones (hardware interno y externo, así como software y redes)

- Interrupciones del transporte (encierros o limitaciones del aeropuerto, encierros del camino, etc.)

Una vez identificados los tipos de desastres la empresa debe seguir y desarrollar un plan para asegurar la viabilidad a largo plazo de la universidad, es necesario que la gerencia se involucre en la elaboración del plan, pero es el Comité de Seguridad de la Información que determina que tipos de planes son aplicables pues se requiere de financiamiento de los mismos.

Las pruebas son útiles si reflejan también condiciones reales y si los resultados de la prueba se utilizan para mejorar el plan.

Es importante comenzar con un plan simple para probar y después aumentar el alcance de la prueba gradualmente. Para cada caso es importante:

- Identifique el alcance y las metas para la prueba.
- Documente el plan de prueba y los resultados.
- Repase los resultados con los participantes y prepare las lecciones aprendidas de la prueba.
- Ponga al día el plan basado en los resultados de la prueba.

Proceso de gestión de la continuidad del negocio

Para sobrevivir, la organización debe asegurar el funcionamiento de aplicaciones criticas en un tiempo razonable, frente a un desastre. Las organizaciones necesitan entrenar a sus empleados para ejecutar los planes de contingencia, para lo cual se requiere:

- Que los empleados sean consientes de la necesidad del plan
- Informar a todos los empleados de la existencia del plan y proporcionar los procedimientos para seguir en caso de una emergencia
- Entrenar al personal con las responsabilidades identificadas para cada uno de ellos, para realizar la recuperación del desastre y procedimientos de continuidad de negocio
- Dar la oportunidad para que se pueda llevar a cabo el plan de contingencia, para poder realizar un simulacro de la forma en la que se ejecuta el mismo.

Desarrollo e implantación de planes de contingencia

Al desarrollar el plan se debe tener bien definido y especificado las responsabilidades ha asignarse a cada persona responsable de un proceso determinado, para el caso de la UPS se debe considerar los siguientes responsables:

- Personal encargado de la administración de la recuperación.- El cual debe actuar el momento en el cual se presente el desastre, y cuyo trabajo consiste en ejecutar el plan de recuperación de desastre y restaurar los procesos críticos en el menor tiempo, para este caso es el Comité de Seguridad.
- Personal operacional. Son aquellos que están encargados de la operación del negocio hasta que las cosas vuelvan a la normalidad, estas personas tienen responsabilidades cotidianas y desarrollan las mismas funciones bajo circunstancias normales.
- Personal de las comunicaciones. Personal que diseña los medios de comunicar la información a los empleados, a los clientes, y al público en general. Son los encargados de considerar qué información puede darse y por quién. Esto es critico en los primeros días de una interrupción pues habrá una mayor demanda para la información, y ocurre en un momento en que los canales normales son interrumpidos por daños en los mismos.

Una vez que se encuentra definido el personal necesario para los diferentes procesos del plan, es necesario que se realicen pruebas del mismo. Pues un plan que no ha sido probado puede presentar fallas en el momento de su ejecución. Las pruebas no deben ser costosas ni interrumpir la operación diaria del negocio. Entre las pruebas que se pueden considerar son:

- Prueba de papel. Esto puede ser tan simple como discutir el plan en una reunión del personal considerando sucesos actuales. Es importante documentar la discusión y utilizar cualquier lección aprendida como parte del proceso para mejorar el plan.
- Camino Estructurado. Aquí es donde el personal define diversos panoramas para supervisar el plan en equipo.
- Prueba de componentes. En esta prueba, cada parte del plan total se puede probar independientemente. Los resultados entonces se miran para considerar cómo el plan total pudo haber trabajado si todos los componentes fueron probados simultáneamente.
- Simulación. No incluye realmente la mudanza a una localización alterna sino puede incluir la simulación de interrupciones para uso general como manera de ver que tan completo es un plan.
- Ejercicio de la recuperación del desastre. En esta prueba, se activa el plan y los sistemas informáticos se cambian a sus sistemas de reserva, que pueden incluir el funcionamiento en los sitios alternativos. Esto a veces se llama una prueba "paralela" pues los sistemas de producción seguirán siendo funcionales mientras que los sistemas de la recuperación se ponen en producción para probar su funcionalidad.

Cumplimiento

Generalidades

Los controles implementados en puntos anteriores deben ser complementados con regulaciones de disposiciones legales y contractuales que están actualmente rigiendo en el país. Pero es necesario definir internamente de forma clara los requisitos normativos y contractuales pertinentes a cada sistema de información de la empresa.

Objetivos

Entre los principales puntos a cubrir se tienen:

- Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al Organismo y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.
- Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad del Organismo.

Alcance

Este control se aplica a todo el personal de la empresa.

Derechos de propiedad intelectual

Es necesario para toda organización conocer las leyes para no tener problemas futuros debido a incumplimiento de las mismas.

La infracción a estos derechos podría dar como resultado acciones legales que derivarían en demandas penales.

Se deberán tener presentes las siguientes normas:

1998: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.

Salvaguarda de los registros de la organización

Los registros críticos de la empresa se deben proteger contra pérdida, destrucción y posibles falsificaciones.

Para un mejor control los registros van a clasificarse dependiendo del área y el uso de cada departamento; además de detallar la forma de almacenamiento, el responsable de cada registro y el periodo de retención, es decir el tiempo que debe transcurrir antes de que sean destruidos.

Es necesario tener presentes las siguientes normas:

2002 - 67: De esta ley se deben considerar diferentes artículos como son:

"Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia."

"Art. 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.... El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo."

Cabe recalcar q en el nuevo decreto ejecutivo del 2009, estos artículos respecto a la ley de comercio electrónico, firmas electrónicas y mensajes de datos no han sido modificados hasta la fecha de tal manera que no ha perdido vigencia el suplemento 557 del 17 de abril del 2002. .

Protección de los datos y de la privacidad de la información personal

Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

Para mejorar este punto, en la empresa se debe redactar Compromiso de Confidencialidad, el cual deberá ser suscrito por todos los empleados.

Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate.

Evitar el mal uso de los recursos de tratamiento de la información

Los recursos de procesamiento de información del Organismo se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

Revisiones de la política de seguridad y de la conformidad técnica

Conformidad con la política de seguridad

Cada Responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

b) Implementación del Plan de Tratamiento de Riesgos

El objetivo de este punto es tomar la acción más apropiada de tratamiento para cada uno de los riesgos identificados, en base al cuadro anterior y al capítulo anterior donde se encontraba la valoración de los riesgos:

ACTIVOS	AMENAZAS	VULNERABILIDADES	PTR
	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Acceso no autorizado a la portátil	Falta de Protección por desatención de equipos	Reducción
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no adecuado del aire acondicionado	Reducción
	Instalación no autorizada o cambios de Software	Falta de control de acceso	Reducción

Hardware Portátil	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados	Reducción
	Uso no previsto	Falta de las políticas	Reducción
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal	Reducción
	Degradación del HW	Falta de mantenimiento adecuado	Reducción
	Inautorizada copia de SW o información propietaria	Falta de políticas	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Robo	Falta de protección física	Reducción
PCs de oficina	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Acceso no autorizado a la portátil	Falta de Protección por desatención de equipos	Reducción
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no adecuado del aire acondicionado	Reducción
	Instalación no autorizada o cambios de Software	Falta de control de acceso	Reducción
	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados	Reducción
	Uso no previsto	Falta de las políticas	Reducción
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal	Reducción
	Degradación del HW	Falta de mantenimiento adecuado	Reducción

	Inautorizada copia de SW o información propietaria	Falta de políticas	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Robo	Falta de protección física	Reducción
Servidores	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Corrupción de archivos de registros	Falta de Protección de los archivos de registro	Reducción
	Negación de Servicio	Incapacidad de distinguir una petición real de una falsa	Reducción
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Reducción
	Acceso no autorizado a través de la red	Código malicioso desconocido	Reducción
	Degradación o Falla del HW	Falta de mantenimiento adecuado	Reducción
	Manipulación de la configuración	Falta de control de acceso	Reducción
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal	Reducción
	Incapacidad de restauración	Falta de planes de continuidad del negocio	Reducción
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)	Reducción
	Brechas de seguridad no detectadas	Falta de monitoreo de los servidores	Reducción
	Ataque destructivo	Falta de protección física	Reducción
Equipos de	Fuego	Falta de protección contra fuego	Reducción

Oficina	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Degradación o Falla de HW	Falta de Mantenimiento	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Uso no previsto	Falta de Políticas Falta de Control de Acceso	Reducción
Soporte electrónico	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Condiciones inadecuadas de temperatura y/o humedad	Susceptibidad al calor y humedad	Aceptación
	Ataque destructivo	Falta de protección física	Reducción
	Robo	Falta de atención del personal	Reducción
	Escape de información	Manipulación inadecuada de información	Reducción
Documentación y	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Pérdida de información	Errores de los empleados	Reducción
	Pérdida de información	Almacenamiento no protegido	Reducción
	Divulgación de información de clientes	Almacenamiento no protegido	Reducción

Registros	Incumplimiento de leyes en cuanto a la información de clientes o empleados	Falta de conocimiento de los empleados	Reducción
	Incorrecta o incompleta documentación del sistema	Falta de documentación actualizada del sistema	Reducción
	Contratos incompletos	Falta de control para el establecimiento de contratos	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Incapacidad de restauración	Falta de planes de continuidad del negocio	Reducción
	Modificación no autorizada de información	Insuficiente entrenamiento de empleados	Reducción
Empleados	Errores de los empleados y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento	Reducción
	Insuficiente personal	Falta de acuerdos definidos para reemplazo de empleados	Reducción
	Divulgación de información confidencial	Falta de acuerdos de confidencialidad	Reducción
Establecimientos	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Acceso no autorizado	Falta de políticas	Reducción
	Acceso no autorizado	Falta de protección física	Reducción
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
Servicio de	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Degradación del servicio y equipos	Falta de mantenimiento adecuado	Reducción

Comunicaciones	Errores de configuración	Falta de conocimiento del administrador	Reducción
	Manipulación de la configuración	Falta de control de acceso	Reducción
	Uso no previsto	Falta de políticas	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Fallas de servicios telefonía	Falta de acuerdos bien definidos con terceras partes	Reducción
Servicio de energía eléctrica	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Reducción
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Ataque destructivo	Falta de protección física	Aceptación
Servicio de correo electrónico	Errores de los usuarios	Falta de conocimiento del uso del servicio	Reducción
	Suplantación de la identidad del usuario	Falta de control de acceso	Reducción
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)	Reducción
	Uso no previsto	Falta de políticas	Reducción
	Fallas de servicios de soporte (telefonía, servicios de Internet)	Falta de acuerdos bien definidos con terceras partes	Reducción
Aplicaciones Internas	Errores de usuarios	Falta de conocimiento para el uso de la aplicación	Reducción
	Errores de configuración	Falta de capacitación del administrador del sistema	Reducción
	Escapes de información	Falta de control de acceso	Reducción
	Errores de actualización del programa	Falta de procedimientos aprobados	Reducción
	Manipulación de la configuración	Falta de control de acceso	Aceptación
	Suplantación de identidad del usuario	Falta de control de acceso	Reducción

	Abuso de privilegios de acceso	Falta de políticas de seguridad	Reducción
	Negación de servicio	Incapacidad para distinguir una petición real de una petición falsificada	Reducción
Portal de información (Página Web de la empresa)	Modificación no autorizada del sitio Web	Falta de procedimientos para cambios	Reducción
	Negación de servicio	Falta de recursos necesarios	Reducción
	Sitio Web no disponible	Fallas en los acuerdos de niveles de servicio	Reducción
	Publicación de información incorrecta de la UPS	Falta de procedimiento aprobados	Reducción
Suministros de Oficina	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Robo	Falta de atención	Reducción
	Robo	Falta de protección física	Reducción
Imagen de la empresa Reputación	Divulgación de datos de los clientes	Insuficiente seguridad de información de los clientes	Reducción
Paquetes o software estándar	Negación de Servicio	Capacidad insuficiente de los recursos	Reducción
	Virus de Computación, Fuerza Bruta y ataques de diccionario	Falta de Protección(AV) actualizada	Reducción
	Spoofing, Escape de información	Falta de control de acceso	Reducción
	Falta de capacidad de restauración	Falta de copias de backup continuas	Reducción
	Uso no previsto	Falta de políticas de seguridad	Reducción
	Negación de Servicio	Capacidad insuficiente de los	Reducción

		recursos	
Sistemas operativos	Errores de Configuración	Falta de capacitación del administrador	Reducción
	Errores de Configuración	Incompleto o incorrecto documentación del sistema	Reducción
	Virus de Computación, Fuerza Bruta y ataques de diccionario	Falta de Protección (AV) actualizada	Reducción
	Falta de capacidad de restauración	Falta de copias de backup continuas	Reducción
	Pérdida de Servicio	Actualizaciones incorrectas	Reducción
	Pérdida de Servicio	Instalación de SW no autorizado	Reducción
	Controles de Seguridad no cumplidos	Falta de Políticas de Seguridad	Reducción
	Alteración no autorizado de la configuración	Falta de control de acceso	Reducción
Medios y soporte	Acceso no autorizado a la información	Falta de control de acceso	Reducción
	Robo	Falta de protección física	Reducción
	Daños de cables	Falta de protección física	Aceptación
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)	Reducción
	Brechas de seguridad no detectadas	Falta de monitoreo de la red	Reducción

Tratamiento de Riesgos

ANEXO 2

Administración de la seguridad en aplicaciones

1- La auditoria incluye un intento controlado de romper los controles de seguridad del sistema por una persona ajena a este?

SI NO

2- Las medidas y políticas de seguridad de la organización están estrictamente aplicadas en los sistemas?

SI – En todos ellos Algunos de ellos
Ninguno de ellos

3- Existe una definición clara de las responsabilidades operacionales, de desarrollo y de entrada de datos entre los miembros?

SI NO

4- Están todos los recursos asignados a un usuario especifico y es su responsabilidad especificar el nivel de protección de los mismos?

Si, con especificación Si, Sin especificación NO

5- El nuevo personal es informado de las políticas/estándares de seguridad y de su responsabilidad en relación a estas?

SI NO

6- Están los usuarios conscientes de la importancia de mantener sus password confidenciales y que será el responsable de cualquier divulgación?

NO Confidencial y responsable
Solo confidencial No aplica

7- Los usuarios saben que no deben dejar una terminal ingresada y desatendida?

SI NO

8- Están los usuarios conscientes que no deben almacenar contraseñas en teclas de función de terminales o en discos con programas de auto ingreso?

SI NO

9- Están los datos fuentes diseñados a un nivel de seguridad o debidamente identificados (para restringir el acceso y/o identificar su sensibilidad)?

No datos Todos los datos Algunos

10- Si existe un software producido fuera de la compañia, se han realizado chequeos para asegurar que la compañia es confiable?. Los contratos han sido cambiados para asegurar la integridad del software?

Chequeos realizados chequeos y contratos
Contratos cambiados ni chequeos ni contratos

11- Esta el sistema completa y adecuadamente asegurados?

Solo reemplazo fisico Pérdida física y funcional
Solo perdidas funcionales Ningun tipo de perdida

Auditoria del sistema

1- El acceso a los registros/archivos está restringido al personal necesario por sus funciones (por defecto seria sin acceso)?

SI NO

2- Que tipo de acceso tiene el auditor para auditar los registros/archivos? Seleccione la opción menos aplicable.

Ninguno Borrado Lectura
Otro Actualización

3- El sistema mantiene un registro de los accesos e intentos de acceso a este (incluye terminales-ids,etc)?

SI NO solo violaciones

4- Que tan a menudo se producen y son revisados los registros por violaciones?
Seleccione la respuesta más apropiada.

Diario o más frecuente Cuando se sospecha de violación
Un día si otro no Nunca
Semanalmente No aplica

5- Es posible auditar y monitorear la actividad de un usuario especifico?

Si No

6- Son los programas más sensitivos auditados individualmente cuando se ejecutan?

Si No

7- La fecha y hora del ultimo ingreso es registrado cuando un usuario ingresa? Estan todos los usuarios instruidos para chequear esto y reportar cualquier discrepancia?

Si No

Contingencia de las aplicaciones

1- Esta la frecuencia de la copia de datos parcial o completamente determinada por las capacidades de recuperación de la aplicación?

No Completa
Parcial No Back-up de datos

2- Existe un mecanismo en el lugar, como un punto de chequeo y restauración, para ayudar en caso de fallas del sistema durante un proceso de datos?

Si No

3- Son los procedimientos de contingencia de aplicaciones y salvaguardas probados y satisfechos:

Regular/Frecuentemente Nunca
Periódicamente No aplica
Rara vez

Contingencia y Back-up

1- Se realizan copias de respaldo regularmente y donde se mantienen?

No
Si – Fuera del sitio

Si – En el sitio
Si – Dentro y fuera del sitio

2- Están las copias especiales (si existen) fuera del sitio?
Si
No

3- Se mantienen copias de la documentación e instrucciones de operación?
No
Si – Dentro y fuera del sitio
Si – En el sitio
No aplica
Si – Fuera del sitio

4- Los respaldos en el sitio, de archivos, programas, documentación e instrucciones de operación están almacenados para prevenir el acceso no autorizado y riesgo de daño (fuego, etc)?
Solo acceso no autorizado
Ambos acceso y daño
Solo riesgo de daño
Ni acceso ni daño

5- Se han asignado responsabilidades individuales para la implementación de cada componente del plan de recuperación y se ha nombrado un coordinador de la recuperación?
Si
Solo un coordinador
No
Solo para cada componente

6- El plan de recuperación debería incluir detalles de todos los requerimientos administrativos y acuerdos. Cuáles de los siguientes, si existe, son omitidos?
Procedimientos obtenidos
Detalles del seguro
Planes financieros

7- Existe un plan de recuperación en un lugar fuera del sitio?
Si
No

8- Los detalles para el reemplazo de equipos han sido formulados, incluyendo costos (unitario y total) y el tiempo de reemplazo de la unidad?
Si
No incluye costos
No
No incluye tiempo

9- Los acuerdos legales obligatorios en el sitio con vendedores incluye soporte de hardware para equipo critico (incluyendo garantías en tiempo de respuesta)?

Si
No

Hardware

1- Cuanto tiempo de servicio fue perdido el ultimo año por fallas de hardware?
0% - 1%
4% - 5%
1% - 3%
Mas de 5%

2- Las siguientes actividades son permitidas en el cuarto de equipos o en las proximidades a dispositivos de hardware?
Fumar
Comer
Beber

3- Existen procedimientos en el sitio para un seguro apagado (y eventual re-inicio) después de una falla de hardware critica detectada?
Si
No

4- Cuantos diferentes vendedores están involucrados en contratos de mantenimiento?

1-2 3-5 mas de 5

5- El mantenimiento preventivo se lleva a cabo regularmente y en fechas predeterminadas?

Si No

6- Todo el trabajo de mantenimiento es documentado y supervisado?

Si No

7- El trabajo de mantenimiento por los vendedores se lleva a cabo en presencia de una o mas miembros del personal permanente?

Si No

8- Que practica es adoptada cuando hardware de almacenamiento tiene que ser removido del sitio por mantenimiento/reparación?

Vaciado de datos sensitivos Ninguno

Acompañamiento del personal No aplica

Ambos

Riesgos

1- Que restricciones de humo existen en el sitio?

Ninguna No se permite fumar en absoluto

2- Que tan frecuente se realizan trabajos en el edificio o se dan alteraciones en el?

A menudo Rara vez

Algunas veces Nunca

3- Cuantos incendios han existido dentro de la instalación en los últimos 5 años? Si son mas de 5 ingrese 5

Numero de incendios →

4- Es el equipo eléctrico apagado cuando no se usa?

SI NO

5- Que tan a menudo son las áreas de computadoras limpiadas a profundidad?

Diariamente Semanalmente

Un dia si otro no Mensualmente

6- Están los detectores de humo presentes a lo largo de la instalación?

Si No

7- Están los detectores de calor/fuego presentes a lo largo de la instalación?

SI No

8- Que tan a menudo son probados los sistemas de detección de humo/calor/fuego?

Regularmente Rara vez

Periódicamente Nunca

9- Son los extintores manuales suficientes para el rango de potenciales incendios (eléctricos, químicos, etc)?

SI No

10- Están los extintores adecuadamente ubicados y marcados claramente?

SI No

11- Están todos los empleados instruidos en el uso de extintores y conocen de los procedimientos y políticas de incendios?

SI No

12- Las paredes alrededor de áreas criticas van desde el sub-piso hasta el super-techo (sobre el techo falso)?

Solo desde el sub-piso — Ninguno
Solo hasta el super-techo — No aplica
Ambos

13- Existen puertas de incendio en el lugar para diseminar el fuego?

Si — No

14- Hay salidas y rutas de evacuación claramente marcadas e identificadas?

Si — No

15- Han ocurrido inundaciones o daños por agua en la instalación:

En los últimos 3 años — Mas de 8 años
3 a 5 años — No en absoluto
5 a 8 años

16- Ha habido una falla de energía en la instalación en los últimos 3 años?

Si — No

17- Existe un regulador de energía y un sistema de monitoreo instalado?

Si — No

18- Cuan a menudo se realiza un mantenimiento preventivo al equipo de UPS y soporte?

Regularmente/a la marcha — Rara vez
Periódicamente — Nunca

19- Puede una falla en la unidad de aire acondicionado causar daño al hardware o resultar en perdida del servicio?

Si — No

20- Cuantas veces el sistema de computo ha sido interrumpido en los últimos dos años debido a una falla en el aire acondicionado?

Numero de interrupciones -->

21- Existe un plan de standy/back-up en caso de una falla prolongada del aire acondicionado?

Si — No

22- Cual de las siguientes, si existe, podria afectar mas seriamente a la instalación o el área en general?

Huracanes /vientos extremos — Tormentas eléctricas
Hundimiento — Nieve pesada/daño de hielo
Inundaciones — Terremotos

23- Es el edificio estructuralmente mas fuerte y construido con materiales no combustibles?

Si — No

24- Cuantos pisos tiene el edificio?

Numero de pisos →

25- Han sido examinados y probados los pisos que contienen equipos de computación y eléctrico para soportar su peso?

Si — No

Redes y Comunicaciones

1- La red es:

Interna a un edificio
Interna a un sitio
En una región geográfica
En un país
En más de un país

2- Cuál es el tipo de conexión a lineas públicas?

Interna PABX o PBX
Compartida PABX o PBX
Línea directa
Otro
No aplica

3- Cuantos nodos hay en la red?

2
3 – 5
6 - 10
11 – 20
Más de 20

4- Que protocolos son usados?

X25/Packet Switched
SDLC/HDLC
Binary Synchronous/9030
LAN/Ethernet/DECNET/TCPIP
Otro

5- Cuantos usuarios tienen acceso al sistema?

Menos de 50
51 a 250
251 a 1000
2001 a 10000
Más de 10000

6- Han sido definidos los requerimientos mínimos en términos de disponibilidad y rendimiento?

SI
NO

7- Que de lo siguiente no ha sido definido en la red?

Enlaces críticos
Equipo critico
Software critico

8- Que facilidades de recuperación de la red existen en el lugar?

Líneas de reserva/adicionales
Rutas alternadas
Ninguna de estas
No aplica

9- Puede una sesión pendiente, ser cancelada fácilmente si una violación de seguridad ha ocurrido o existe la sospecha?

Si
No

10- Para tener acceso a la red/sistema, todos los usuarios deben ingresar al menos un usuario y password, un password junto con tarjeta, una representación con un dispositivo biométrico, u otro valor similar único?

Si
No

11- El identificador del terminal es siempre transmitido al acceder al sistema?

Si
No

12- Se usa un mensaje técnico de autenticación?

Si
No
Solo Datos/Sistema seleccionado
No aplica

13- El sistema previene la transmisión de mensajes/datos sensitivos a nodos y terminales indefinidos o inválidos?

Si
No

14- Cuan viejo es el equipo de comunicaciones en promedio?

Menos de 2 años
Menos de 5 años
5 a 8 años
Mas de 8 años

15- Cual fue el porcentaje de tiempo fuera debido a fallas de red/comunicación se dio durante los últimos 12 meses?

Menos de 1% Mas de 3%
1 – 3%

16- Esta el equipo de prueba y diagnostico para unidades de lineas/comunicaciones lista y disponibles?
Si No

17- Existe una transmisión de datos sensitiva o confidencial?
Si No

18- Los datos transmitidos son encriptados?
Todos No
Solo datos seleccionados

19- Cual es el primer medio usado para transmisión?
Cobre/Par trenzado Satelite/microonda
Coaxial Cable Fibra óptica
Otro

20- El acceso al circuito de red y sus diagramas de configuración es estrictamente controlado y limitado a aquellos que lo requieren?
Si No No aplica

21- En lo posible los multiplexores, switches y otros equipos de comunicación sensitivos están localizados en áreas seguras?
Si No No aplica

22- Que tan frecuentemente se reasignan puertos en la instalación?
Muy frecuentemente Raramente
Frecuentemente Nunca
Algunas veces No aplica

23- Las asignaciones y reasignaciones de puertos están correctamente registradas y documentadas?
Si No No aplica

24- El nivel de trafico de la red es monitoreado?
Si No No aplica

25- Se transmiten mensajes de registro de ingreso?
Si No
Depende de la aplicación

Acceso Fisico

1- Que tan cercano es el acceso del público a la instalación?
Muy cerca al edificio Acceso al sitio pero no al edificio
Acceso al edificio No cercano al edificio

2- Existe un parqueadero de autos sobre o bajo la instalación del edificio?
Si No

3- El sitio/locación ha sido sujeto a manifestaciones, desordenes civiles, riñas, etc?
Si No

4- Cuál es la percepción en general del público sobre la instalación?
Apreciada por la comunidad Publico no conoce sobre su función
Indeseable Combinación de ambos

5- Ubicación exacta de la instalación?

Base/sótano del edificio — Construcción del centro de computo
Planta baja — Adecuada
1ero/2do piso — Otro
3er piso o sobre el edificio

6- Cuantas entradas/salidas existen para el ingreso y salida de la instalación (además de las de emergencia)?

Ninguna — Una
Dos — Tres
Más de tres

7- Qué sistema de acceso mecánico/eléctrico existe en el lugar durante las horas laborales?

Dispositivo Biométrico — Seguro y llave de sistema
Sistema tarjeta/Tacto — Ninguno
Seguro con combinación

8- Todas las puertas y ventanas externas están alarmadas?

Si — No

9- Los controles de acceso físico son probados e inspeccionados regularmente (incluyendo test de intento de acceso no autorizado)?

Si — No

10- Quien debe llevar insignias de identificación?

Nadie — No-empleados
Empleados — Empleados y No-Empleados

11- Cuando una persona relevante con autorizaciones deja la organización, que de los siguiente no se realiza. Seleccione lo aplicable a la instalación?

Cambio de seguros — Eliminación de tarjeta
Cambio de combinaciones — Recuperación de la insignia

12- Los controles de acceso también aplican al personal de servicio (limpieza, proveedores, etc.)?

Si — No — No aplica

13- Para terminales que desplieguen datos altamente sensitivos, estas son:

Standard — Plasma
LCD — No aplica

14- El movimiento de medios (magnéticos, reporte sensitivos, etc.) hacia y desde la instalación es estrictamente controlado y registrado?

Si — No

15- Los chequeos de inventarios se realizan para:

Medios magnéticos — Ambos
Salida sensitiva/documentación — Ninguno

Administración de la seguridad

1- El rol y función de la administración del sistema de seguridad está definido y separado de otras?

Si — Diferente pero no definido
No — Definido pero no diferente

2- Existe un control dual/mecanismo de validación en el lugar para cambios en las reglas de acceso a recursos?

Si No No aplica

3- Puede el administrador de la seguridad tener acceso a contraseñas activas (si un usuario olvida su clave)?

Si No No aplica

4- El acceso al sistema está controlado por el uso de users-ids?

Si No

5- Cada acceso individual al sistema tiene un user-id único, o hay users-id compartidos?

Los user-ids son individuales Algunos user-id son compartidos

6- Cuando un id de usuario es creado o su clave es reseteada, como se comunica la nueva contraseña al usuario?

Este es estándar y conocido En persona
Por teléfono Otro/combinación de estos
Por carta

7- Cuando una nueva clave es emitido por el administrador de seguridad o del sistema, esta expira automáticamente cuando se usa por primera vez (forza al usuario a cambiarla)?

Si No No aplica

8- Los id de usuario y clave son removidos cuando un miembro del equipo es transferido o deja la organización?

Si Solo en terminación laboral
No Desconoce
Solo en transferencia

9- Es necesario una solicitud formal por escrito de la administración antes de que un nuevo usuario sea configurado?

Si No

10- Existe un "super-usuario" o "especial" y esta imitado al mínimo numero de usuarios que lo requieren para su función?

Si No con tales atributos
No

11- El acceso al sistema está controlado por claves?

Si No

12- Como se escogen los passwords?

Por el usuario Generada por el sistema
Por el gerente Otro
Por el administrador de seguridad

13- Se requiere una autorización formal para el cambio/creación de contraseñas?

Si Solo creación
No Solo cambio

Administración de la seguridad

1- La política de seguridad esta detallada y completamente documentada?

Si No
Si, pero no documentada

2- La política de seguridad y los programas para conocerla concierne al personal de TI y de oficina?
Si Solo personal de Ti
Solo usuarios Ni usuario ni personal de Ti

3- Algunas de las siguientes áreas no están cubiertas por la política de seguridad?
Software de aplicación Procedimientos de oficina
Software de sistema Redes (si aplica)
Datos Hardware/Equipo de oficina

4- La política de seguridad deberá cubrir disponibilidad, autenticidad, confidencialidad, correcto funcionamiento e integridad. Todos estos están cubiertos?
Si No

5- Las auditorias de seguridad son detalladas y conducidas en periodos regulares?
No Si, por un Dep. Independiente
Si, por este departamento Si, por consultores externos

6- Que aspectos/partes de un sistema son normalmente incluidos en la auditoria?
Desarrollo/operación software Ambos
Solo procedimientos de oficina Ninguno de estos

7- Las politicas y medidas de seguridad son estrictamente forzosas?
Si No

8- Existe una clara delimitación entre las responsabilidades del grupo de trabajo en lo referente a operación, desarrollo e ingreso de datos?
Si – Todos ellos Ninguno de ellos
Algunos de ellos

9- Existen un especialista a cargo de la tarea de coordinar la seguridad y asegurar que las politicas sean comunicadas apropiadamente?
No Solo comunicación
Solo coordinación Ambos

10- Los gerentes saben de su responsabilidad sobre la seguridad dentro de sus dominios?
Si No

11- EL nuevo personal está informado de las políticas/estándares de seguridad y de su responsabilidad con ellas?
Si No

12- Existe un programa en proceso para incrementar la conciencia de seguridad (posiblemente incluya cartas y seminarios/cursos)?
Si No

13- Existen reglas en el lugar para la elección de contraseñas? Longitud minima de 5 caracteres, la elección obvia debe ser eliminada, etc.
Si No No aplica

14- El mal uso de recursos esta estrictamente definido y prohibido (no juegos, desarrollos "privados", etc.) y existe software para restringirlo?
Si, con software de control No
Si, No software de control

15- Contratos con cualquiera de los siguientes no incluye una clausula directamente relacionada con responsabilidades de seguridad?

Agencia/contratante de staff	Ingenieros/Personal mantenimiento
Vendedores/Proveedores	Personal permanente

16- Hay un nivel de seguridad asignado a todos los usuarios?

Si	No

17- Se realizan chequeos específicos para asegurar que el sistema cumpla con la legislación local/internacional (servicios financieros, etc.)

Si	No	No aplica

18- La seguridad u otra política estipula convenciones de nombre para id de usuarios, transacciones, programas, archivos de datos? Indique cualquiera aplicable pero no cubierto:

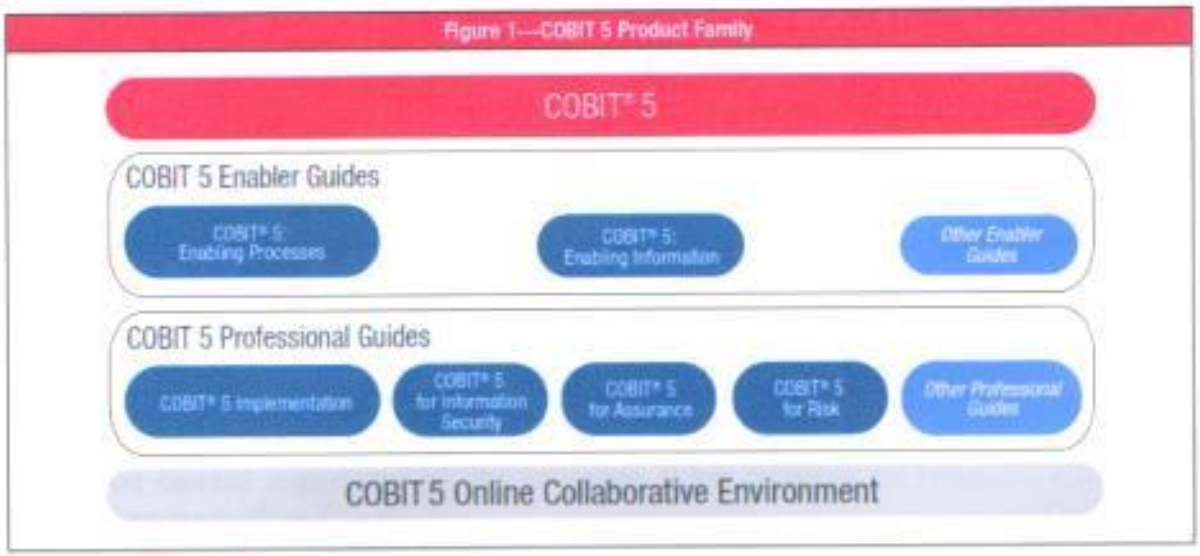
User-ids	Programas/Módulos
Transacciones	Archivos de Datos

Anexo 3

Como parte del capitulo 1 se expone la actualización que viene con el marco de referencia del COBIT 5.0, a continuación en el grafico a se expone la familia de productos de esta versión

Grafico A

Familia de Productos del COBIT 5.0



Como se mencionó anteriormente, se debe crear el ambiente adecuado para garantizar el éxito de la iniciativa de la implementación o mejora. El ciclo de vida y sus siete fases siete ilustran en la figura B

Grafico B

El ciclo de vida y sus siete fases

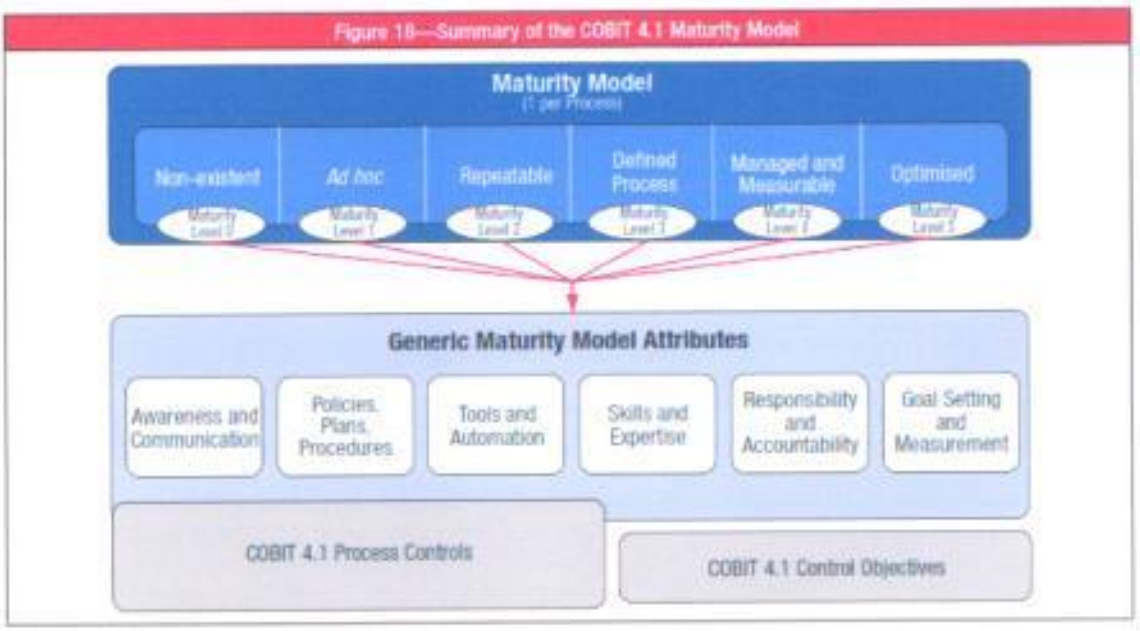
Figure 17—The Seven Phases of the Implementation Life Cycle

Existe un cambio importante en los procesos y los modelos de madurez que se expresa en las graficas C y D

Grafica C

Modelo de Madurez del Cobit

Figure 18—Summary of the COBIT 4.1 Maturity Model



Grafica D

Modelo de referencia de los procesos del Cobit 5.0